SPRINGER NATURE
Reference

Lauren R. Shapiro
Marie-Helen Maras
Editors

Encyclopedia of Security and Emergency Management

Springer

Encyclopedia of Security and Emergency Management

Lauren R. Shapiro • Marie-Helen Maras
Editors

Encyclopedia of Security and Emergency Management

With 53 Figures and 38 Tables

Springer

Editors
Lauren R. Shapiro
Department of Security, Fire, and Emergency Management
John Jay College of Criminal Justice
City University of New York
New York, NY, USA

Marie-Helen Maras
Department of Security, Fire, and Emergency Management
John Jay College of Criminal Justice
City University of New York
New York, NY, USA

ISBN 978-3-319-70487-6 ISBN 978-3-319-70488-3 (eBook)
ISBN 978-3-319-70489-0 (print and electronic bundle)
https://doi.org/10.1007/978-3-319-70488-3

© Springer Nature Switzerland AG 2021
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedication

To my parents, Lawrence and Irma Shapiro,
For your years of endless guidance, support, and love –
thank you

To my beloved niece and goddaughter, Phoebe Maras
Follow your dreams and make them a reality

Preface

National and international security concerns have considerably evolved. Globalization has triggered growing and exponential threats that challenge the security and stability of countries by transcending traditional borders and having a transnational impact. To understand these security threats and the ways to counter them, a multidisciplinary approach to their examination is required. This encyclopedia was written to fill the void by comprehensively covering various facets of security through a multidisciplinary lens of criminology, criminal justice, sociology, psychology, law, police studies, political science, history, risk, computer science, management, and public policy and administration. Particularly, this encyclopedia provides students, academics, and practitioners in a wide range of fields with comprehensive and contemporary information on security. The topics range from security threats (e.g., cybercrime, terrorism, shoplifting, and fraud) to both applications on the job and coordination between public and private sectors in handling security and emergency situations nationally and internationally. The chapters cover security concepts, methods, functions, theories, organizations, and technology; the history and current state of the discipline; security measures (i.e., physical security, personnel security, and cybersecurity); critical infrastructure protection; emergency management; and public-private partnerships. The encyclopedia will serve as a resource allowing readers to learn best practices in security; understand weaknesses in current techniques; develop risk assessment skills; predict vulnerability in a range of businesses and critical infrastructure sectors (e.g., healthcare, energy, water, dams, financial, commercial, and government facilities, communications, and information technology sectors, to name a few); and implement mechanisms for managing natural and human-made disasters.

Acknowledgments

We would like to extend our warm thanks to Ruth Lefèvre at Springer for her direction and assistance during the development and production of this encyclopedia.

Our gratitude is extended to all of the authors for their contributions and reviewers (listed below) for their valuable insight to ensure that the encyclopedia contained comprehensive, excellent material.

Reviewers

Alex Alexandrou, Chelsea Binns, Robert Matthiessen, Robert D. McCrie, Susan Pickman, Robert Till, Lucia Velotti, and Hung-Lung Wei

List of Topics

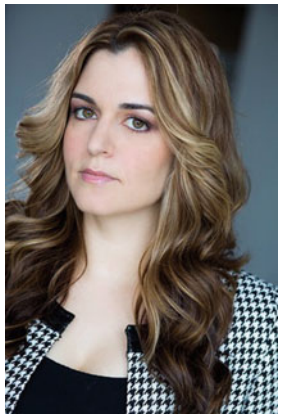
Airport Security: Incidents That Changed Procedures
Airport Security: Procedures in Secured Areas for TSA and Private Security
American Society for Industrial Security (ASIS)
Arrest
Big Data
Biometrics
Border Security
Bribery
Bus Security
Business Continuity Plan
Celebrity Protection
Corporate Security
Criminals: Active Shooters
Criminals: Blue-Collar Crimes
Criminals: Cybercriminals
Criminals: Motives
Criminals: Suggestions to Improve Security Procedures
Criminals: Terrorists
Criminals: White-Collar Crimes
Critical Infrastructure: Commercial Facilities Sector
Critical Infrastructure: Critical Manufacturing Sector
Critical Infrastructure: Defense Industrial Base Sector
Critical Infrastructure: Emergency Services Sector
Critical Infrastructure: Government Facilities Sector (GFS)
Critical Infrastructure: Nuclear Reactors, Materials, and Waste Sector
Critical Infrastructure: Transportation Systems
Critical Infrastructure: Water and Wastewater Systems Sector
Critical Infrastructure Protection
Cultural Institutions Security
Cybersecurity: Incident Response
Cybersecurity: Policy
Cybersecurity: Practice
Cybersecurity: Preparedness
Data Protection
Department of Homeland Security (DHS)
Drones
Educational Institution Safety and Security
Emergency Management: Best Practices
Emergency Management: Crisis Communication
Emergency Management: Crisis Management and Response
Emergency Management: Evacuations
Emergency Management: Incident Command System
Emergency Management: Infant and Young Children Feeding in Emergencies
Emergency Management: International
Emergency Management: Pets
Emergency Management: Preparedness and Planning
Emergency Management: Recent Incidents That Contributed to Changes in Emergency Management Legislation and Procedures
Emergency Management: Recovery

Emergency Management: Shelter In-Place
Emergency Management: Spontaneous Volunteers in Response to Disaster
Emergency Management: Working with Vulnerable Populations
EU Private Security Regulation
Event Security
Executive Protection
Federal Emergency Management Agency
Fire: Evacuation (Engineer Solutions)
Fire: Prescriptive and Performance Based Design
Fire: Prevention, Protection, and Life Safety
First Responders: Police
Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
Geographic Information Systems (GIS) Applications in Emergency Management
Hazardous Environmental Effects
HAZMAT
Health Security: Securing Borders and Managing COVID-19
Homeland Security Act of 2002
Human-Made Disasters: Electric Power and Transit Linked Outages
Human-Made Disasters: Toxic Waste and Residences
Industrial Control System
Influence of Risk Perception on Event Risk Management and Decision-Making
Insider Threat
Intelligence
Internet of Things
Internet (Deep and Dark Web)
Interviewing Adults: Communication at the Front Line
Interviewing Children
Intrusion Detection Systems
Investigations: Accidents and Reconstructions
Investigations: Bank Fraud
Investigations: Burglary
Investigations: Consumer Retail Shoplifting
Investigations: Criminal
Investigations: Cybercrimes
Investigations: Domestic
Investigations: Employee Theft of Employer Property
Investigations: Environmental Pollution Dumping
Investigations: Firearms
Investigations: Fraud
Investigations: Money Laundering
Investigations: Negligence
Investigations: OSHA
Investigations: Polygraph Use
Investigations: Sexual Assault
Investigations: Terrorism
Investigations: Use of DNA and Fingerprints
Law: Administrative
Law: Specialized
Machine Learning
Maritime Security: Acceptable Risks
Maritime Security: Armed Guards on Board
Maritime Security: Contraband
Maritime Security: Problems of Security Versus Safety Practices
Mercenary and Private Military
Natural Hazards
Natural Hazards: Earthquakes
Natural Hazards: Floods
Natural Hazards: Hurricanes, Cyclones, and Typhoons
Natural Hazards: Pandemic Threats by Infectious Diseases
Natural Hazards: Tornadoes
Natural Hazards: Tsunamis
Natural Hazards: Volcanic Eruptions
Personnel Security: Hiring
Personnel Security: Recruitment
Personnel Security: Retention
Personnel Security: Selection
Personnel Security: Training
Physical Security: Best Practices
Physical Security: Exterior Application
Physical Security: High-Rise Residence and Office Buildings
Physical Security: Interior Applications
Physical Security: Methods and Practices
Physical Security: Video Surveillance, Equipment, and Training
Police: Public Versus Private Policing
Private Detectives

Protection and Security in Public Spaces
Public-Private Partnerships: Port Security
Public-Private Partnerships: Security Organizations
Public-Private Partnerships: Training and Coordination in Disasters
Rail (Train) Security
Residential Security: Gated Communities
Residential Security: Houses and Apartments, Public and Private
Retail Security: Employee Theft
Retail Security: Shoplifting
Retail Security: Use of Security Guards
Risk Analysis: National and International Standards
Robots
SCADA
Security Guards: Academic and Training Programs
Security Guards: Authority and Power
Security Management
Security: Concepts and Definitions
Security: Contract
Security: Hybrid
Security: Private
Security: Proprietary
Security: Theories
Terrorism: Domestic
Terrorism: Homegrown
Terrorism: International
Tort: Property
Workplace: Hostile Environment
Workplace: Privacy
Workplace: Sexual Harassment
Workplace Violence: Active Shooter/Terrorist Threats
Workplace Violence: Assault
Workplace Violence: Factors Contributing and/or Facilitating
Workplace Violence: Intimate Partner Violence
Workplace Violence: Past and Current Employees
Workplace Violence: Sex-Related Crimes

About the Editors

Dr. Lauren R. Shapiro is an Associate Professor in the Department of Security, Fire, and Emergency Management at John Jay College in New York. Her Ph.D. is in Developmental Psychology from Rutgers University, and she also has an M.S. in Criminal Justice from Indiana University, an M.S. in Experimental Psychology from Ohio University, and a dual B.A. in Psychology and in Early Childhood Education from the University of Buffalo. Dr. Shapiro was a Postdoctoral Research Fellow at the Carolina Consortium on Human Development at the University of North Carolina, Chapel Hill. She served as an Extern with the Honorable Ralph Erickson in the US District Court of North Dakota, Fargo, and as an Intern with the Fargo Police Department. Dr. Shapiro has certificates from the Royal Canadian Mounted Police in First Responder Terrorism Awareness (core program) and from the City of Fargo ND in Child Custody Investigator. She teaches professional training workshops and certificate courses for justice and security professionals. Dr. Shapiro consults with psychologists, attorneys, and officials in the police, sheriff, and district attorney departments and has been interviewed about her work by television and newspaper journalists. She is the co-author of *Multidisciplinary Investigation of Child Maltreatment* (Jones and Bartlett, 2016) and author of *Cyberpredators and Their Prey* (CRC Press), which should be available next year. Her research, which focuses on various issues in physical security, border security, private investigation, cyber security, and school safety and security, has been presented at national and international conferences and published in journals and books.



Dr. Marie-Helen (Maria) Maras is an Associate Professor at the Department of Security, Fire, and Emergency Management at John Jay College of Criminal Justice. She is also part of the faculty of the M.S. program in Digital Forensics and Cybersecurity at John Jay College of Criminal Justice and the Ph.D. program in Criminal Justice at the CUNY Graduate Center. Dr. Maras has a DPhil. in Law and an MPhil in Criminology and Criminal Justice from the University of Oxford. In addition, she holds a graduate degree in Industrial and Organizational Psychology from the University of New Haven and undergraduate degrees in Computer and Information Science and Psychology from UMUC. She is the author of *Cybercriminology* (Oxford University Press, 2016); *Computer Forensics: Cybercriminals, Laws, and Evidence* (now in its second edition; Jones and Bartlett, 2014); *Counterterrorism* (Jones and Bartlett, 2012); *CRC Press Terrorism Reader* (CRC Press, 2013); and *Transnational Security* (CRC Press, 2014), among other publications. Prior to her academic post, she served in the US Navy for approximately seven years, gaining significant experience in security and law enforcement from her posts as a Navy Law Enforcement Specialist and Command Investigator. During the early stages of her military career, she worked as an Electronics and Calibration Technician.

Contributors

Shannon N. Abbott Center for Global Security and Cooperation, Sandia National Laboratories, Albuquerque, NM, USA

Yalcin Acikgoz Department of Psychology, Appalachian State University, Boone, NC, USA

Halil Akbas Troy University, Troy, AL, USA

Alex Alexandrou John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Rifath Ali Department of Safety, Security, and Emergency Management, College of Safety and Justice, Eastern Kentucky University, Richmond, KY, USA

Peter Ashwin Event Risk Management Solutions, Boise, ID, USA

Mathieu Auger-Perreault Cybersecurity, Georgia Institute of Technology, Atlanta, GA, USA

Lynne E. Baker-Ward Department of Psychology, North Carolina State University, Raleigh, NC, USA

John Balestrieri John Jay College of Criminal Justice, City University of New York, New York, NY, USA

John T. Bandler Bandler Law Firm PLLC and Bandler Group LLC and John Jay College of Criminal Justice, New York, NY, USA

Jennifer Bencivenga John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Navneet Bhushan Crafitti Consulting, Bengaluru, India

Chelsea A. Binns John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Sara Bonati SAGAS, Università degli studi di Firenze, Florence, Italy

David J. Brooks Security Science, School of Science, Edith Cowan University, Perth, WA, Australia

R. Bull University of Derby, Derby, UK

Mark Camillo Security, Fire and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Madeline Carr Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), University College London, London, UK

Kevin A. Cassidy Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Paolo Cavaliere University of Delaware, Newark, DE, USA

Christopher A. D. Charles Department of Government, University of the West Indies, Mona, Jamaica

Frank Chen John Jay College of Criminal Justice, New York, NY, USA

Constantine (Dean) K. Christakos Columbia University, New York, NY, USA

Alex Chung Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), University College London, London, UK

Christopher Cleary St. John's University, New York, NY, USA

Maira Compagnone Department of Psychology, Appalachian State University, Boone, NC, USA

Michael P. Coole Security Science, School of Science, Edith Cowan University, Perth, WA, Australia

Keith Cozine College of Professional Studies, St. John's University, Queens, New York City, NY, USA

G. Dalton Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

Sneha Dawda Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), University College London, London, UK

Mark DeMario John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Sarah E. DeYoung University of Georgia, Athens, GA, USA

Jared R. Dmello Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Christopher Dowling Australian Institute of Criminology, Canberra, ACT, Australia

James M. Duggan Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Michael A. Edgerton HudsonTrident., Inc, Camden, NJ, USA

Yarin Eski Knowledge Hub Security and Societal Resilience/Political Science and Public Administration, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Ashley K. Farmer Illinois State University, Normal, IL, USA

Lusiella Fazzino St. John's University, Jamaica, NY, USA

James J. F. Forest Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Kevin R. Gamache Texas A&M University, College Station, TX, USA

Anthony Gentile Security, Fire, and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA

Gary A. Gordon Emergency Management Department, Massachusetts Maritime Academy, Buzzards Bay, MA, USA

Kevin Govern Ave Maria School of Law, Naples, USA

George Grispos School of Interdisciplinary Informatics, University of Nebraska Omaha, Omaha, NE, USA

Kenneth J. Grossberger John Jay College of Criminal Justice, New York, NY, USA

Zakir Gul Criminal Justice Department, State University of New York (SUNY), Plattsburgh, NY, USA

Duygu Biricik Gulseren Department of Psychology, Saint Mary's University, Halifax, NS, Canada

Harald Haelterman Faculty of Law and Criminology – Department of Criminology, Criminal Law and Social Law, Ghent University, Ghent, Belgium

Wim Hardyns Institute for International Research on Criminal Policy (IRCP), Ghent University, Ghent, Belgium

Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Antwerp, Belgium

Devon Hickman Department of Psychology, Appalachian State University, Boone, NC, USA

Hua-Lun Huang Department of Sociology, Anthropology, and Child and Family Studies, University of Louisiana, Lafayette, LA, USA

Atif Hussain Systems Security Group, Institute for Future Transport and Cities (FTC), Coventry University, Coventry, UK

M. Nazrul Islam Farmingdale State College, State University of New York, Farmingdale, NY, USA

John M. Jelenek Security Department, NewYork-Presbyterian Hospital, New York, NY, USA

Bernard A. Jones Division of Criminal Justice, Legal Studies and Homeland Security, College of Professional Studies, St. John's University, Jamaica, NY, USA

E. Kevin Kelloway Department of Psychology, Saint Mary's University, Halifax, NS, Canada

Brian P. Kelly Security Systems and Law Enforcement Technology, Farmingdale State College, Farmingdale, NY, USA

Brian Kohlhepp John Jay College of Criminal Justice, New York, NY, USA

Detective Sergeant, Ross Township Police, Pittsburgh, PA, USA

M. M. Laske Department of Psychology, Appalachian State University, Boone, NC, USA

Seungmug (Zech) Lee Department of Criminology and Criminal Justice, The University of Texas at Arlington, Arlington, TX, USA

Michael K. Lindell Department of Urban Design and Planning, Institute for Hazards Mitigation Planning and Research, University of Washington, Seattle, WA, USA

Adriane C. Littlefield Center for Global Security and Cooperation, Sandia National Laboratories, Albuquerque, NM, USA

Peter Mameli Public Management, John Jay College of Criminal Justice, New York, NY, USA

Marie-Helen Maras Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Amanda W. Martin University of North Carolina, Chapel Hill, NC, USA

Ronald L. Martin Capital Technology University, Laurel, MD, USA

Robert Matthiessen Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

B. May Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

Robert McCrie Department of Security, Fire and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA

David A. McEntire College of Health and Public Service, Utah Valley University, Orem, UT, USA

Clarissa Meerts Faculty of Law, Department of Criminal Justice and Criminology, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

R. Milne Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

Jennifer Mincin Health and Human Services Department, SUNY Empire State College, Selden, NY, USA

Michelle D. Miranda Farmingdale State College, The State University of New York, Farmingdale, NY, USA

Anthony Morgan Serious and Organised Crime Research Lab, Australian Institute of Criminology, Canberra, ACT, Australia

Gwynn Morris Department of Psychology, Meredith College, Raleigh, NC, USA

Veronika Nagy Willem Pompe Institute for Criminal Law and Criminology, Utrecht University, Utrecht, The Netherlands

J. Nunan Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

Kenneth W. O'Donnell John Jay College of Criminal Justice, New York, NY, USA

Lisa C. Orloff Worldcares, New York, NY, USA

Heather A. Panter Centre for Advanced Policing Studies, Liverpool John Moores University, Liverpool, UK

E. Parrott Liverpool John Moores University, Liverpool, UK

Arie Perliger School of Criminology and Justice Studies, Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Sidra Perveen King Edward Medical University, Lahore, Punjab, Pakistan

Susan Pickman John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Pierre-Luc Pomerleau Business Administration – Homeland Security and Leadership Policy, Northcentral University, San Diego, CA, USA

Koen Ponnet Department Communication Sciences, imec-mict-Ghent University, Ghent, Belgium

Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Antwerp, Belgium

Tim Prenzler School of Law, University of the Sunshine Coast, Sunshine Coast, QLD, Australia

Troy Rawlins Department of Safety, Security, and Emergency Management, College of Safety and Justice, Eastern Kentucky University, Richmond, KY, USA

Joshua Reichert Fire Protection and Paramedicine Sciences, Eastern Kentucky University, Richmond, KY, USA

Malcolm B. Reid College of Graduate and Continuing Studies, Norwich University, Northfield, VT, USA

Genserik Reniers Safety and Security Science Group, TU Delft, Delft, The Netherlands

Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Antwerp, Belgium

Carlos E. Restrepo Tandon School of Engineering, New York University, New York, NY, USA

Nagaraj S. V. School of Computing Science and Engineering, VIT, Chennai, India

Douglas E. Salane Mathematics and Computer Science Department, John Jay College of Criminal Justice, New York, NY, USA

Jamie Sanderson Reid Thomson Reuters, Richmond, VA, USA

Marlies Sas Research group on Law Enforcement and Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Antwerp, Belgium

Emily Schindeler Griffith Criminology Institute, Griffith University, Brisbane, QLD, Australia

Paul J. Schmick Alliance Security, New York, NY, USA

Dorothy Moses Schulz Law, Police Science, and Criminal Justice Administration, John Jay College of Criminal Justice (CUNY), New York, NY, USA

Siraj Ahmed Shaikh Systems Security Group, Institute for Future Transport and Cities (FTC), Coventry University, Coventry, UK

Lauren R. Shapiro Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

A. Shawyer Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK

Thomas Shea Police Graduate Studies Program, College of Education and Human Services, South Orange, NJ, USA

Brian Keith Simpkins Homeland Security Program, Eastern Kentucky University, Richmond, KY, USA

Sonny Smith Texas A&M University, College Station, TX, USA

Trevor A. Smith University of the West Indies, Mona, Jamaica

Anna Stamper Homeland Security, Disaster and Emergency Management, Eastern Kentucky University, Richmond, KY, USA

Veronica Strandh Department of Political Science, Umeå University, Umeå, Sweden

William J. Sullivan Homeland Security, Eastern Kentucky University, College of Justice and Safety, Richmond, KY, USA

Matthew M. Sweeney School of Criminology and Justice Studies, University of Massachusetts Lowell, Lowell, MA, USA

Tabatha Thibault Saint Mary's University, Halifax, NS, Canada

Denise D. P. Thompson Department of Public Management, John Hay College of Criminal Justice, The City University of New York, New York, NY, USA

Spyridon Triantafyllou John Jay College of Criminal Justice, New York, NY, USA

Lisa van Reemst Department of Criminology, Erasmus School of Law, Erasmus University Rotterdam, Rotterdam, The Netherlands

Lucia Velotti Department of Security, Fire and Emergency Management, City University of New York (CUNY), John Jay College of Criminal Justice, New York City, NY, USA

Adam Scott Wandt John Jay College of Criminal Justice, New York, NY, USA

Haiden Weaver Department of Psychology, Appalachian State University, Boone, NC, USA

Hung-Lung Wei Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, CUNY, New York, NY, USA

Adam D. Williams Center for Global Security and Cooperation, Sandia National Laboratories, Albuquerque, NM, USA

Darien A. Williams Massachusetts Institute of Technology, Cambridge, MA, USA

Richard R. Young School of Business Administration, Capital College, The Pennsylvania State University, Middletown, PA, USA

Rae Zimmerman Institute for Civil Infrastructure Systems, Robert F. Wagner Graduate School of Public Service, New York University, New York, NY, USA

A

Airport Security: Incidents That Changed Procedures

Heather A. Panter
Centre for Advanced Policing Studies,
Liverpool John Moores University,
Liverpool, UK

Keywords
Terrorism · Skyjackings · Hijackings · Airplane bombings · Airport security

Definition

A security incident that changed security procedures is defined by the involvement of the following essential components: hijacking, skyjacking for ransom, attempted bombings/bombing incidents on planes, and/or attacks on airport structures themselves. In respect to hijacking, a hijacking is the seizure of a plane's control by force or threat of force. Skyjacking is the kidnapping of passengers of an airplane by threats of force for ransom whether monetary or political. Besides the historical analysis of these crimes and forms of terrorist activities targeted at commercial aviation, this entry describes how specific security incidents influenced airport security procedures.

Introduction

Modern aviation is favored as a target for attacks because of its vulnerabilities and human, psychological, and economic repercussions. Notably, planes are highly visible targets that are readily associated with specific nations, and a successful attack generates a large number of causalities with a high level of press coverage. Further, commercial aircraft are often regarded as "symbols of Western technological prowess" (Chow et al. 2005, p. 3). Hence why hijackers and bombers alike often target them. Proactively, security tactics have evolved to address specific techniques used during attacks. Often these changes are a direct result of specific incidents that commercial aviation has had to face. Examining timelines of attacks upon commercial aviation, there are distinct tactical phases both pre-9/11 and post-9/11. With each distinct phase, the tactics of attackers caused procedural changes in commercial airport security.

Pre-9/11

Nitroglycerin Carry-On Luggage Bombings (1933–1960s)

The first commercial plane bombing occurred on October 10, 1933, on a United Airlines Boeing

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

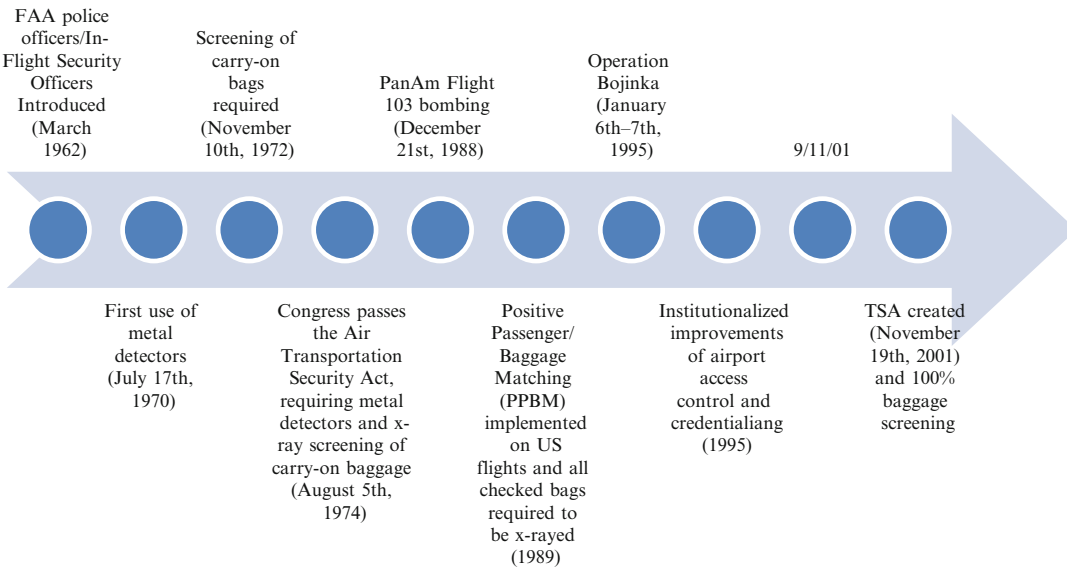
247 (Van der Linden and Seely 2011). The case remains unsolved today, but it is suspected that the nitroglycerin bomb was a result of a Chicago gang murder plot (Van der Linden and Seely 2011). While this incident did not lead to changes in security procedures, it was a litmus test for how future bombings would be carried out on commercial airlines (refer to Fig. 1), namely, packing dynamite in suitcases and carrying it aboard via passenger luggage [see Canadian Pacific Air Lines (1949), Kashmir Princess (1955), United Airlines Flight 629 (1955), National Airlines Flight 967 (1959), and National Airlines Flight 2511 (1960)].

Creation of Air Marshals (1960s–Current)

In 1961, Antuilo Ramierez Ortiz used a gun to force the flight crew of a National Airlines jet to divert to Cuba and thus became the first US hijacker (Department of State 2006). This incident, along with the hijacking epidemic occurring during the time, leads to the creation of the first air marshal program. In March 1962, in-flight security began with the US Federal Aviation Administration introduction of FAA Peace Officers who covertly traveled on planes to combat airline skyjackings (Elias 2009). These FAA Peace Officers, or known worldwide as In-Flight Security Officers (IFSOs), were the first people to provide armed security onboard commercial aircraft. Since their institution to commercial airliners, the FAA has handed security duties to the TSA. Internationally, covert in-flight surveillance has been in operation after FAA implementation [Australia (2001), Austria (1981), Canada (2002), India (1999), Ireland (1970s), Pakistan (1976), United Kingdom (2003), etc.].

"Golden Age" of Skyjacking and Passenger Screening (1970s–1980s)

By 1970, hijackings reached epidemic proportions with 118 incidents of unlawful aircraft seizures and 14 incidents of sabotage/armed attacks against commercial airlines (Price and Forrest 2016). Screening passengers and carry-on baggage started in the early 1970s as a way to deter hijackings that was regulated by airline industries themselves. This often led to subcontracted screenings by vendors with the lowest bid (Price and Forrest 2016). As such, screening companies had high turnover rates with staff often under-


FAA police officers/In-Flight Security Officers Introduced (March 1962)
First use of metal detectors (July 17th, 1970)
Screening of carry-on bags required (November 10th, 1972)
Congress passes the Air Transportation Security Act, requiring metal detectors and x-ray screening of carry-on baggage (August 5th, 1974)
PanAm Flight 103 bombing (December 21st, 1988)
Positive Passenger/ Baggage Matching (PPBM) implemented on US flights and all checked bags required to be x-rayed (1989)
Operation Bojinka (January 6th–7th, 1995)
Institutionalized improvements of airport access control and credentialiang (1995)
9/11/01
TSA created (November 19th, 2001) and 100% baggage screening

Airport Security: Incidents That Changed Procedures, Fig. 1 Pre-9/11 Security Reactive Measures Timeline

qualified (Price and Forrest 2016). This led to several airport security failures.

Notably, prior to the introduction of standardized regulations, passenger screening for guns and hand grenades (the most common tactics at the time) leads to a reduction of airline incidents, and thus, the evolution of security screening programs halted due to financial demands placed upon airliners combined with a reduction of hijackings. At the time, the financial cost of security screening often superseded any proactive security desires. So private airlines and airports, which were responsible for providing security, often relied upon minimal cost-effective measures that were reactive instead of effectively proactive.

Strategically during this time, airline acts of sabotage remanded consistent with either a bomb concealed in checked-in baggage, body-worn explosives, or body-worn handguns. Yet, criminal tactics changed, and airlines/airports had to reconsider their cost-prohibitive security attempts. On November 10, 1972, hijackers (Melvin Cale, Louis Moore, Henry D. Jackson, Jr.) threatened to fly Southern Airways Flight 49 into a nuclear reactor in Oak Ridge Tennessee (Department of State 2006). This was the first time when a plane was attempted to be used as a weapon. Strategically, this highlighted how the failure of adequate passenger screening could have a larger destructive impact financially, politically, and psychologically to airline acts of sabotage globally. This particular significant incident could be arguably be connected to the similar tactic used by 9/11 hijackers.

Shortly before takeoff from Birmingham, Alabama, Southern Airway Flight 49 hijackers produced handguns and hand grenades and took over the commercial flight with 34 people onboard demanding $10 million (Price and Forrest 2016). During the 30-hour hijacking, hijackers had the plane make multiple stops in the USA and Canada while threatening to fly into the High Flux Isotope Reactor at the Oak Ridge National Laboratory (Naftali 2009). During negotiations with the FBI, officials only managed to get between $2 and $2.5 million of ransom money while landed in Chattanooga, Tennessee (Naftali 2009). If successful in crashing the plane into the nuclear reactor, the nuclear fallout would have been arguably as devastating as Chernobyl. The hijackers then set course for Havana, Cuba, but Cuban leader Fidel Castro refused their admittance into the country; therefore, the plane was flown to Orlando, Florida, to refuel. The FBI shot out two of the four tires of the plane, and the hijackers shot the copilot while ordering the plane to take off again to Cuba (Naftali 2009). Once landed in Cuba, the hijackers were removed via gunpoint by Cuban authorities. This specific incident, combined with other hijackings, leads to an emergency ruling by the US Federal Aviation Administration to mandate screening of all passengers and inspect carry-on luggage (Yoo and Choi 2006). With this incident, along with the increasing international political unrest, the FAA recognized the strategic need to expand and improve security screening despite previous cost operative tactics.

FAA Introduction of Explosive Detection Canine Teams (1972)

When TWA Flight 7 departed New York's JFK airport, the airline was notified that a bomb was hidden onboard. Since, bomb threats were so common, it took 10–15 min to determine if the threat was a hoax (Witkin 1972). The flight was redirected back to JFK and was promptly evaluated. During the subsequent plane search, a bomb-detecting K-9 discovered a device in the jetliner's cockpit minutes before it was set to detonate (Witkin 1972). The device was hidden in a black suitcase and was constructed of C-4 (plastic military explosive), which went undetected by metal detectors used during preflight screening. Notably, the FAA recognized that the current usage of x-ray and metal detector technologies was insufficient in detecting plastic explosives, and they sought more effective detection methods. As such, this specific incident led to the creation of the FAA Explosive Detection Canine Team Program. Notably, K-9 bomb detectors are faster, more versatile, reliable, and more cost-effective than conventional instrumental detection methods (see Furton and Myers 2001).

Deliberate Sabotage and IED Suitcase Bombings (1980–1990s)

Pan Am Flight 103

From the 1960 to 1970s, security focus changed from hijackings toward detecting deliberate sabotage in the 1980–1990s (Fobes et al. 1995). Notably, on December 21, 1988, a suitcase bomb on Pan Am Flight 103 killed 244 passengers, 15 crewmembers, and 11 residents on the ground in Lockerbie, Scotland (Elias 2009). Following a lengthy investigation, it was determined that two Libyan nationals (arrested in November 1991) with the assistance of Libyan intelligence officer Abdelbaset al-Megrahi (arrested in 2001) were identified as the bombing suspects. Libyan leader Muammar Gaddafi also accepted responsibility in 2003 and paid compensation to the victims despite his contradictory claim that he did not give the order to attack. Because of this incident, positive passenger/baggage matching (PPBM) became a regulatory responsibility in the USA for international flights (Elias 2009). Previously, baggage could be checked onto flights without a corresponding passenger. Further, US carriers at European and Middle Eastern airports required PPBM matched baggage to undergo x-ray and hand searches of all checked baggage after Pam Am Flight 103 bombing.

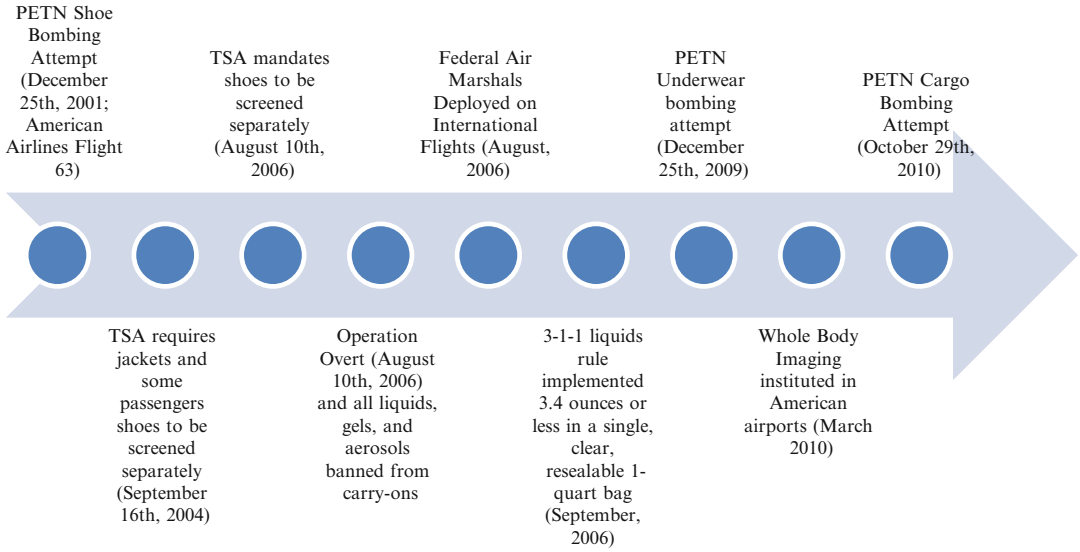
PSA Flight 1771

Strategically, bomber tactics changed from checked baggage bombs back to carry-on baggage devices. This was a direct result to the countermeasures that were instituted after Pam Am Flight 103. On January 6–7, 1995, Ramzi Yousef and two Al-Qaeda coconspirators were foiled in the bombing attempts of 12 US commercial airliners on international routes (Operation Bojinka). Yousef's Cell had planned to use liquid-based explosives that were undetectable by the screening technologies currently in use at airports (Price and Forrest 2016). Notably, had the bombing plot been successful, the death toll would have been one of the most devastating terrorist attacks upon commercial airlines. Because of this incident, development of additional policies and procedures, specifically airport access control and credentialing (i.e., badging and background checks), was instituted. Further, because of this failed mass-bombing incident, Khalid Sheikh Mohammed (considered to be the architect of the 9/11 attacks) decided to tactfully move away from explosives and to use airplanes themselves as weapons.

Post 9/11 Attacks (Person-Borne IEDs)

Prior to September 11, 2001, airport screening was provided by private agencies contracted through airlines or airports. On September 11, 2001, hijackers Khalid al-Mindhar, Nawaf al-Hazmi, and Salem al-Hazmi set off metal detectors during preflight screening. CCTV video of the footage showed that they had what appeared to be box cutters attached to their back pockets. Notably, box cutters and small knives were at the time allowed to be carried aboard aircraft. Using box cutters and suspected faux body bombs, four planes were hijacked (two crashed into the twin towers of the World Trade Center, one crashed into the Pentagon, and the fourth plane crashed into a field in southern Pennsylvania) which killed over 3,025 US citizens and other nationals. (The death count continues to increase from responders/volunteers who have contracted 9/11-related cancers, pulmonary diseases, mental health stress-related conditions, and other medical conditions. It is anticipated that more responders will die from these illnesses by the end of 2018 than those actually killed on 9/11 (Never Forget Project 2018).)

Two months after the September 11 attacks, US lawmakers made airport security a federal issue by standardizing pre-boarding screening procedures through the creation of the TSA (Transportation Security Agency). Part of this standardization of pre-boarding security processing leads to the banning of certain carry-on items and stricter screening that was continuous federally in the USA (refer to Fig. 2). Other changes included the restriction of non-ticketed individuals into secured passenger areas, fortified aircraft cockpits, TSA's Federal Flight Deck Officers Program (arming crewmembers), and 100% checked baggage screening.


PETN Shoe Bombing Attempt (December 25th, 2001; American Airlines Flight 63)
TSA requires jackets and some passengers shoes to be screened separately (September 16th, 2004)
TSA mandates shoes to be screened separately (August 10th, 2006)
Operation Overt (August 10th, 2006) and all liquids, gels, and aerosols banned from carry-ons
Federal Air Marshals Deployed on International Flights (August, 2006)
3-1-1 liquids rule implemented 3.4 ounces or less in a single, clear, resealable 1-quart bag (September, 2006)
PETN Underwear bombing attempt (December 25th, 2009)
Whole Body Imaging instituted in American airports (March 2010)
PETN Cargo Bombing Attempt (October 29th, 2010)

Airport Security: Incidents That Changed Procedures, Fig. 2 Post 9/11 Attacks (Rise in Aircraft Bombing Attempts with Person-Borne Explosives) Timeline

Internationally, following 9/11, Annex 17 was adopted by the International Civil Aviation Organization (ICAO) Council to address challenges posed to civil aviation (International Civil Aviation Organization 2011). This amendment included new provisions in airport security operations, international cooperation relating to threat information, national quality control, access control at airports, measures related to passengers and their cabin and hold baggage, in-flight security personnel and protection of the cockpit, code-sharing/collaborative arrangements, and management of response to acts of unlawful interference (International Civil Aviation Organization 2011).

PETN Christmas Day Shoe Bomber (2001)

Despite the security measures that were put into place by ICAO, suspects quickly responded by shifting to onboard suicide attacks with concealed person-borne IEDs (Improvised Explosive Device). On December 25, 2001, Al-Qaeda member Richard Reid wore shoes which contained undetected pentaerythritol tetranitrate (PETN) aboard a flight. Pentaerythritol tetranitrate (PETN) is a powerful explosive, which is part of the same chemical family as nitroglycerin and is rarely detectable with conventional "single beam" x-ray machines (see Wells and Bradley 2012). Manufactured as a white powder, it is often a component of plastic explosives like Semtex. It is relatively stable and used primarily as a high explosive. During American Airlines Flight 63, Reid unsuccessfully attempted to detonate the explosive while using triacetone triperoxide (TATP) as a detonator (Wells and Bradley 2012). With this unsuccessful attack, shoes were required to be screened separately, and suspects switched to camouflaging containers filled with liquid explosives.

Operation Overt (2006)

On August 2006, British authorities disclosed that they had interdicted planned attacks of ten transatlantic flights with liquid explosives carried in their hand luggage. MI5 conducted an investigation called Operation Overt where they broke into a flat being used by Ahmed Ali and hid cameras and microphones. Through their surveillance, MI5 determined that Ahmed Ali and Tanvir Hussain were constructing IED devices out of drink bottles. Both suspects experimented with introducing liquid explosives via a syringe into an empty soft drink bottle. The suspects also planned to use a disposable camera for IED parts

and hid an altered AA battery that would be a detonator in carry-on baggage. The disposable camera in question was intended to provide an electrical charge to the detonator that would be strapped to the bottle filled with liquid explosives. This leads to security measures that limited the amount of liquids, aerosols, and gels allowed in carry-on luggage (Wells and Bradley 2012). Further, this significant incident influenced the development and implementation of effective mass-screening technology that better detects explosive liquids (Wells and Bradley 2012). Notably, adjusted security measures restricted the quantity of liquids that people could take aboard aircraft, suspects altered the paradigm once more with the underwear bombing using a device with no metal components.

PETN Underwear Bomber (2009)

On December 25, 2009, an Al-Qaeda extremist (Umar Farouk Abdulmutallab) attempted to detonate an IED concealed in his underwear while aboard a flight from Amsterdam to Detroit (USA) (Bunker 2011). Inside Abdulmutallab's underwear was 80 g (2.8 oz.) of PETN (Bunker 2011). According to intelligence officials, Ibrahim al-Asiri, the chief bomb-maker for Al-Qaeda in the Arabian Peninsula (AQAP), created the device. This leads to the TSA introducing whole-body imaging to security screening procedures in March 2010. Further, laptops and tablets were required to be removed from hand baggage for better screening (see Wetter 2013), the implementation of enhanced pat-downs by TSA officials, and restrictions on cargo occurred due to this incident. Notably, suspects took advantage of metal detector weakness of their failure to detect organic materials comprising of liquid and plastic explosives (Sweet 2009), including TATP, C4/PE4, and PETN.

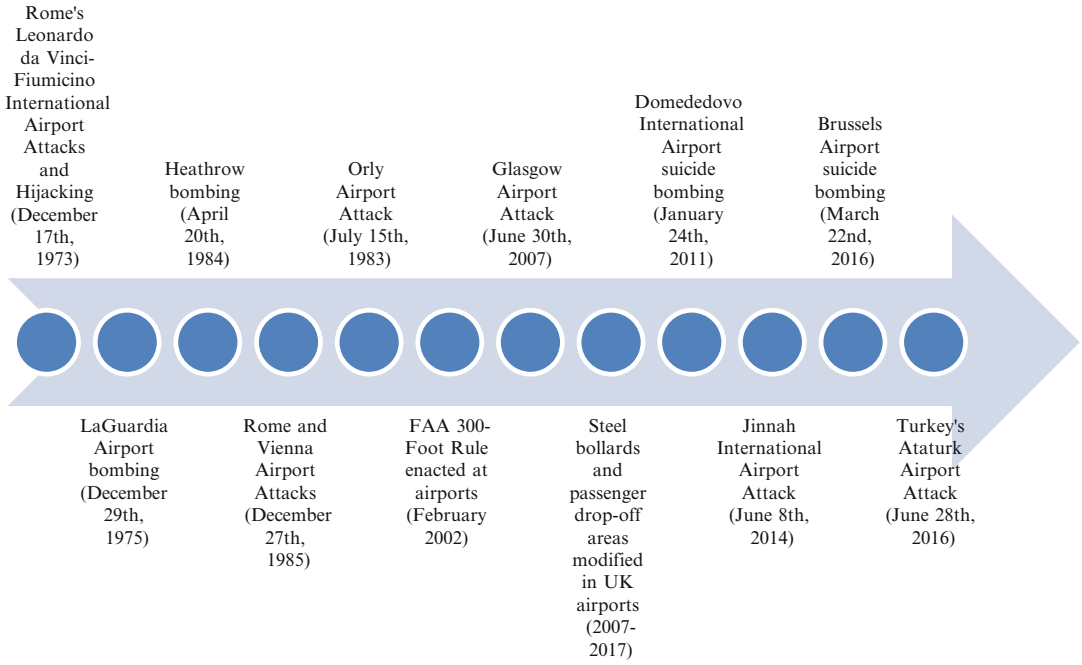
PETN Cargo Bombing Attempt (2010)

Both the raised concerns of a potential internal carrier bomber and the increase in security measures in response to the underwear bombing, AQAP decided to attack cargo aircraft with IEDs hidden in printer toner cartridges. On October 29, 2010, IEDs were found aboard separate cargo flights as a result of intelligence from Saudi Arabia's security chief (Bunker 2017). The IEDs were discovered at stopovers from Yemen at East Midlands (UK) and Dubai (UAE). Both devices where posted in Yemen with freight firms UPS and FedEx with shipping addresses to former locations of two synagogues in Chicago. Reports stated that the devices were meant to detonate midair over US cities (see Bunker 2017). Notably, Yemen does not have regularly scheduled cargo flights, and the suspects likely knew the IEDs would end up on passenger planes as over 50% of airfreight to the USA is transported in the cargo hold of passenger planes (see Rayner and Gardham 2018). The IEDs on both cargo planes were concealed in printer cartridges inside Hewlett-Packard HP desktop laser printers. The printers contained an electrical circuit connected to a mobile phone SIM card and the printer cartridge contained 14 oz. of PETN. Through the investigation of the incident, it was determined that Anwar al-Awlaki was responsible for the attempt with Ibrahim al-Asiri, the chief bomb-maker for AQAP, responsible for the construction of the device. Notably, Ibrahim al-Asiri's IED devices have been reported as being used in the 2009 Christmas Day bomb plot, the 2010 cargo bomb plot, and the May 8, 2012, terror plot.

Because of the PETN Christmas Day Shoe Bomber (2001), Operation Overt (2006), PETN Underwear Bomber (2009), and the PETN Cargo Bombing Attempt (2010), TSA deployed over 500 Advanced Imaging Technologies units, or whole-body imaging, to screen for both non-metallic and metallic threats. Additionally, TSA instituted "enhanced" secondary screening for passengers who decline WBI screening techniques. During this time, TSA implements the Secure Flight program which cross-checks passenger names against a watch list of known or suspected terrorists (see ► "Airport Security: Procedures in Secured Areas for TSA and Private Security").

Attacks on Airport Structures (1973–Current)

As a fundamental problem of aviation, security revolves around the best way to allocate scarce


Rome's Leonardo da Vinci-Fiumicino International Airport Attacks and Hijacking (December 17th, 1973)
Heathrow bombing (April 20th, 1984)
Orly Airport Attack (July 15th, 1983)
Glasgow Airport Attack (June 30th, 2007)
Domededovo International Airport suicide bombing (January 24th, 2011)
Brussels Airport suicide bombing (March 22nd, 2016)
LaGuardia Airport bombing (December 29th, 1975)
Rome and Vienna Airport Attacks (December 27th, 1985)
FAA 300-Foot Rule enacted at airports (February 2002)
Steel bollards and passenger drop-off areas modified in UK airports (2007-2017)
Jinnah International Airport Attack (June 8th, 2014)
Turkey's Ataturk Airport Attack (June 28th, 2016)

Airport Security: Incidents That Changed Procedures, Fig. 3 Airport attacks timeline

resources to reduce the probability of a successful attack, terrorism tactics shifted from the sky, which was being regulated with tighter security (see Fig. 2), to ground attacks. Strategically, with the introduction of passenger and baggage screening, terrorists adapted their approach to specifically attack airport infrastructures themselves (refer to Fig. 3). As airport infrastructures pose unique security vulnerabilities, they have become more attractive, easier, and cause significant financial impact. For example, Chow et al. (2005) theorized that the downing of an airliner via shoulder-fired missile would lead to an economic loss more than $15 million. Stewart and Mueller (2014) further theorized that airport infrastructure attacks (like those highlighted in Fig. 3) can cost over $30 billion in airline losses.

2007 Glasgow Airport Attack via Vehicle

On June 30, 2007, a terrorist used a Jeep Cherokee filled with propane canisters in a ramming attack, which resulted in a fire. Luckily, security bollards outside the entrance stopped the vehicle from entering the terminal (Price and Forrest 2016). Yet, when the vehicle failed to drive through the terminal, terrorist Bilal Abdullah threw petrol bombs from the passenger seat of the vehicle (Brocklehurst 2017). The other terrorist and driver, Kafeel Ahmed, was set alight during the fire and baggage handler John Smeaton kicked Ahmed in the groin subduing him while helping an injured victim (Brocklehurst 2017). For his actions, John Smeaton was awarded the Queen's Gallantry Medal and became a cult hero in Scotland. Notably, several other heroes that day (off-duty police, airport employees, passengers, and cab drivers) assisted in the thwarting of the attack. From a security perspective, new carports and drop-off and pick-up zones were installed which reduced the flow of vehicle traffic near the airport in an effort to deter future terminal attacks. Additionally, other UK airports either blocked off roads that approached terminal buildings or rerouted traffic while introducing more blockades policed by local forces.

Conclusion

As indicated in this entry, significant incidents, crimes, and forms of terrorism have affected and evolved security measures at commercial airports. Arguably, more has been done in since 9/11 from a security standpoint than all the previous years of commercial aviation combined. Further, as these incidents indicate terror cells constantly adapt their tactics to circumvent current security screening procedures. From passenger carried guns and hand grenades, baggage bombs, person-worn IEDs, using lanes as weapons, to attacks on airport structures themselves reactive security measures shifted focus with each changing tactic. Adaptive security measures included improved passenger and baggage screening, PPBM, K-9 bomb detection, Sky marshals, and federalization and improved regulation of screening procedures. With each distinct phase, the tactics of attackers caused procedural changes in commercial airport security.

Cross-References

- ▶ Airport Security: Procedures in Secured Areas for TSA and Private Security
- ▶ Criminals: Terrorists
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Physical Security: Interior Applications

References

Brocklehurst, S. (2017). The day terror came to Glasgow Airport. *BBC News*. Retrieved on 4 Oct 2018 from https://www.bbc.co.uk/news/uk-scotland-40416026

Bunker, R. (2011). *The projected Al Qaeda use of body cavity suicide bombs against high value targets.* Occasional paper. GroupIntel.com, pp. 1–55.

Bunker, R. (2017). *Laptop bombs and civil aviation*. Abu Dhabi: Trends Institution.

Chow, J., Chiesa, J., Dreyer, P., Eisman, M., Karasik, T. W., Kvitky, J., Lingel, S., Ochmanek, D., & Shirley, C. (2005). *Protecting commercial aviation against the shoulder-fired missile threat* (No. RAND/OP-106). Santa Monica: Rand Corp.

Department of State. (2006). *Significant terrorist incidents, 1961–2003: A brief chronology.* U.S. Department of State. Retrieved on 22 Sept 2018 from http://fas.org/irp/threat/terror_chron.html

Elias, B. (2009). *Airport and aviation security: US policy and strategy in the age of global terrorism*. Boca Raton: CRC Press.

Furton, K. G., & Myers, L. J. (2001). The scientific foundation and efficacy of the use of canines as chemical detectors for explosives1. *Talanta, 54*(3), 487–500.

Fobes, J. L., McAnulty, D. M., & Klock, B. A. (1995). *Aviation Security Human Factors Test and Evaluation Master Plan for the Airport Demonstration* (No. A-2001009-94-U-10078). NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

International Civil Aviation Organization (ICAO). (2011). *Annex 17 to the Convention on International Civil Aviation – Safeguarding Civil Aviation Against Acts of Unlawful Interference* (9th ed.). Montreal: ICAO.

Naftali, T. (2009). *Blind spot: The secret history of American counterterrorism*. New York: Basic Books.

Never Forget Project. (2018). *Statistics from 9/11 and 15 years later*. Retrieved on 26 Sept 2018 from http://neverforgetproject.com/statistics/

Price, J., & Forrest, J. (2016). *Practical aviation security: predicting and preventing future threats*. Butterworth-Heinemann.

Rayner, G., & Gardham, D. (2018). Cargo plane bomb plot: Al-Qaeda terrorists 'threatened another Lockerbie'. *Telegraph.co.uk*. Retrieved on 22 Sept 2018 from https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8100970/Cargo-plane-bomb-plot-al-Qaeda-terrorists-threatened-another-Lockerbie.html

Stewart, M. G., & Mueller, J. (2014). Cost-benefit analysis of airport security: Are airports too safe? *Journal of Air Transport Management, 35*, 19–28.

Sweet, K. (2009). *Aviation and airport security: Terrorism and safety concerns* (2nd ed.). Boca Raton: CRC Press.

Van der Linden, F. R., & Seely, V. J. (2011). *The Boeing 247: The first modern airliner*. Washington, DC: University of Washington Press.

Wells, K., & Bradley, D. A. (2012). A review of X-ray explosives detection techniques for checked baggage. *Applied Radiation and Isotopes, 70*(8), 1729–1746.

Wetter, O. E. (2013). Imaging in airport security: Past, present, future, and the link to forensic and clinical radiology. *Journal of Forensic Radiology and Imaging, 1*(4), 152–160.

Witkin, R. (1972). Bomb found on Jet. Here after demand. *The New York Times*. Retrieved on 28 Oct 2018 from https://www.nytimes.com/1972/03/08/archives/bomb-found-on-jet-here-after-2million-demand-bomb-found-on-twa.html

Yoo, K. E., & Choi, Y. C. (2006). Analytic hierarchy process approach for identifying relative importance of factors to improve passenger security checks at airports. *Journal of Air Transport Management, 12*(3), 135–142.

Further Reading

Baum, P. (2016). *Violence in the skies: A history of aircraft hijacking and bombing*. Chichester: Summersdale Publishers.

Bunker, R. J., & Flaherty, C. (2013). *Body cavity bombers: The new martyrs. A Terrorism Research Center book*. Bloomington: iUniverse.

Maguire, M., Frois, C., & Zurawski, N. (Eds.). (2014). *Anthropology of security: Perspectives from the frontline of policing, counter-terrorism and border control*. London: Pluto Press.

Airport Security: Procedures in Secured Areas for TSA and Private Security

Heather A. Panter
Centre for Advanced Policing Studies, Liverpool John Moores University, Liverpool, UK

Keywords

Airport security · TSA · Security screening

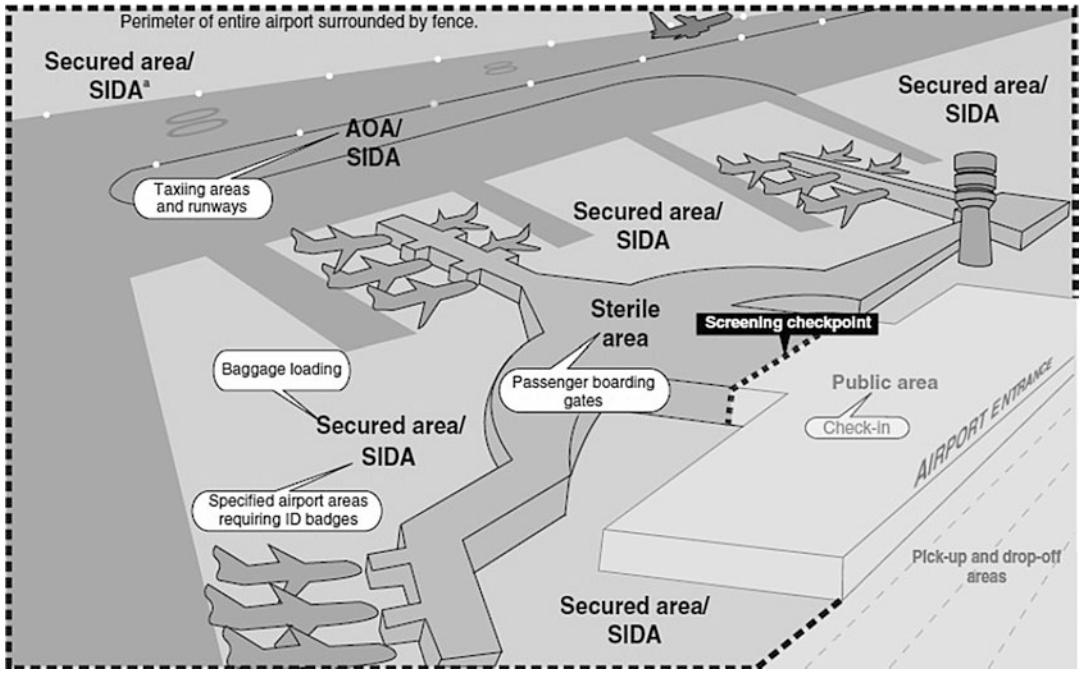
Definition

This entry explores security procedures in secured areas of airports and how governmental and private sectors intersect. Procedures in airport security have to address threats in public/nonpublic areas, in perimeter airfield locations, and within terminals. Often the private sector, with governmental oversight, screens passengers, employees, baggage, and cargo in both secured and nonsecured areas of the airport. Therefore, this entry will examine how both governmental and private security sectors regulate SIDA badge areas, credentialing systems, airport access control, airfield patrol functions, and perimeter security in secure areas of airports.

Introduction

Pre 9/11, private industry fulfilled a more substantial role in commercial transport security as airlines and airports relied solely upon private security contracts. Two months after 9/11, Congress enacted the Aviation and Transportation Security Act (ATSA), Public Law 107-71. This created the Transportation Security Administration (TSA), which federalized commercial passenger and baggage screening. Further, ATSA mandated that 100% of checked passenger baggage was screened (US Congress 2001). With new federalized regulations, private passenger screeners were hired, trained, and employed by the TSA, which became part of the Department of Homeland Security (Price and Forrest 2016). After the passage of ATSA, federal workers replaced contracted private security screeners in 450 commercial airports nationally, and the number of screeners went from 12,000 to over 40,000 in 1 year (Price 2018). Notably, ATSA outlined that TSA's primary function is to ensure regulatory compliance with airport and airline security regulations, to screen passengers, to screen bags, and to deter individuals from committing unlawful acts of interference with aviation (Price and Forrest 2016). DHS's other primary responsibilities also include information analysis and infrastructure protection; chemical, biological, radiological, nuclear (CBRN), and related countermeasures; border and transportation security; emergency preparedness and response; and coordination with other parts of the federal government, with state and local governments, and with the private sector (TSA 2006).

With augmented federalization of airport security, this lead to an altered reliance upon support from private sectors. This reliance shifted from private security agencies being responsible for most secured areas of airports to a radical shift of a blended integration with federalized agencies in security-related research and support. Currently, private sectors aid federalized security in passenger screening, personnel screening, airport access control, credentialing systems, perimeter monitoring, intelligence collection, alarm response, and detection technologies (Price 2018). This integrated merger lead to a layered intersectional approach to airport security procedures.



Airport Security: Procedures in Secured Areas for TSA and Private Security, Fig. 1 Diagram shows secured divisions of typical commercial airport. (Taken from Rabkin et al. (2004))

Presently, security procedures in airports involve the incorporation of shared responsibilities between airport operators, air carriers, private security agencies, local police jurisdictions, federal police jurisdictions, and the Transportation Security Administration (TSA). This layered approach involves distinct security procedures that occur in both unsecured (non-sterile) and secured (sterile) areas within international airports (refer to Fig. 1). Within this layered approach, there are different security threats that are addressed differently, namely, internal threats and external threats. Internally, personnel are concerns within sterile areas. Externally, criminal acts and acts of terrorism are strategic security concerns in sterile areas. As such, there are various components of airport security in sterile areas. This includes screening of passengers and carry-on luggage for weapons and explosives, screening of checked baggage and cargo for explosives, controlling access to sterile areas, clearing and badging personnel with access to both SIDA and AOA areas, and oversight of FAA inspections. Drawing upon tactics used in sterile areas (controlled by security regulating bodies), this entry examines how these current procedures uphold security in sterile areas.

SIDA (Security Identification Display Area) and Air Operation Area Restrictions

Before examining how security layering works in international airports, the first step in understanding airport security is to identify and distinguish non-sterile and sterile boundaries within an airport. A sterile area of the airport is an area that allows passenger access to boarding aircraft, and access is controlled by TSA or an aircraft operator under 49 CFR 1544 or 49 CFR 1546 if a foreign air carrier (Price and Forrest 2016). The purpose of a sterile area located prior to boarding aircraft is to provide a passenger containment area which

prevents persons from gaining access to weapons or contraband after passing through security checkpoint screening (TSA 2006).

FFA regulation Part 107, Section 205, outlines how Security Identification Display Areas (SIDA) are distinguished and regulated within sterile areas. Further, FFA regulation 107.205 authorizes airport operators to carry out measures to prevent unauthorized presence and movement in SIDA locations, establish a personnel identification system, subject each individual to employment history verifications before authorizing unescorted access to SIDA areas, and train each individual before granting unescorted access to SIDA locations. Under Title 49 CFR Part 1542, airport security policies and regulations further regulate (a) access to secured areas and sterile areas of the airport, (b) the requirement that airport personnel wear an approved access/identification badge, (c) the requirement that airport personnel challenge individuals who are not wearing the proper badge (or any badge) in security areas, and (d) the requirement that individuals maintain a proper escort of other individuals who do not have access/ID in a security area.

Monitoring of Employee Movement Through SIDA/AOA Areas

It is often a false conception that all airport employees undergo security screening before entering a sterile area (see Price 2018). Many airport workers in the United States are not subjected the same screening process as airline passengers, but instead they undergo background and criminal history checks, are issued SIDA/AOA badges, and use access-controlled doors to enter sterile areas (see 49 CFR 1542.207), where a credential check is needed. SIDA/AOA badges identify and document when workers enter/exit SIDA sterile areas in airports. Currently, American airports have debated whether all SIDA/AOA badge holders should go through the passenger screening process. As such, some airports have established screening checkpoints at airfield access gates, but private contractors working for the airport conduct employee screening, not the TSA (Price and Forrest 2016). As such, an employee's job responsibility determines their level of access authority and their level of access through access-controlled doors or physical access control systems (PACS). PACS can include locks on a keyed door, keypad locks on doors to more advanced computerized systems with integrated closed-circuit television (CCTV) with alarmed access points (Price 2018). Most of these systems are proprieties of private companies, which develop both hardware and software to manage employee access with federal oversight (Price 2018).

Functionally, only one employee at a time can use the said doors, and SIDA/AOA badges are used as encoded keys that either restrict or permit employees to pass through regulated doors. For example, emergency personnel have access (if SIDA/AOA verified) to all areas contained within sterile areas. This includes SIDA locations and Air Operations Areas (AOA), which are any location where planes land, take off, or surface manoeuver (i.e., runways, taxiways, and aprons). Yet, other members of staff who clean planes or work in catering areas may only have access to certain portions of SIDA or AOA (see Fig. 2). For some, i.e., emergency personnel with SIDA/AOA access, emergencies often supersede screening from a regulatory perspective. Yet, regulated airport access-controlled doors prevent unauthorized personnel from entering sterile areas without undergoing screening even with SIDA badge access.

By controlling who has access to which area, there is an extra security barrier in these sterile areas to reduce internal threats. Examples of internal threats within the sterile area would include the transportation of narcotics, bombing access, and burglary/larceny access to passenger areas and airplanes. By requiring a criminal background check to obtain a secured area ID, airports are arguably reducing the probability of criminality in secured areas. For example, if a prospective employee has an identified criminal history of

Secured/ Security Identification Display Area (SIDA)	Air Operation Area (AOA)	Sterile Area
All workers must display ID badges	If SIDA, all workers must display badges	All workers must display badges
Worker fingerprint checks prior to being granted unescorted access authority	If SIDA, worker fingerprint checks prior to being granted unescorted access authority	Worker fingerprint checks prior to being granted unescorted access authority
Workers not required to be physically screened before entering these areas	Security awareness training for workers	Workers must be physically screened before entering this area; however, alternative approaches can be used
Measures to detect and respond to unauthorized presence in this area	Measures to detect and respond to unauthorized presence in this area	
Signs at access points and perimeters that warn against unauthorized entry	Signs at access points and perimeters that warn against unauthorized entry	
Access control used that meet performance standards (e.g. personal identification number)		

Airport Security: Procedures in Secured Areas for TSA and Private Security, Fig. 2 Security requirements in a typical commercial airport. (Adapted from Rabkin et al. (2004))

theft, then the SIDA process can reduce the probability of granting them access to a tempting area for theft (i.e., non-CCTV areas where baggage is stored, duty-free items, alcohol, etc.).

Screening Technology Used Prior to Entering Sterile Areas

There are four major screening areas before admittance into any sterile areas of the airport: passengers, carry-on baggage, hold baggage, and cargo. In respect to passenger screening, Enders, Sandler, and Cauley's (1990) evidence-based research over the effects of metal detector screening in airports found that they reduce incidents of aerial hijacking. Gabbidon et al. (2012) further found that the usage of x-ray technologies has effectively led to a dramatic decrease in the number of aircraft hijackings. Lum et al. (2006) found that when examining security, target-hardening strategies at airports through increased detection are an effective type of intervention. Constantly evolving, these target-hardening strategies (e.g., metal detectors, airport screening, whole-body imaging, etc.) have evolved since the height of airline skyjackings since 1961.

Prior to 1972, private security officers contracted through airports and airlines performed hand searches for baggage brought aboard airplanes (Wetter 2013). With the increase in air traffic and the number of air passengers, efficiency demands changed. With the invention and adaptation of x-ray imaging of baggage during security screening, later developments of imaging technologies, more sophisticated training, and certification for x-ray screeners in airport security checkpoints screening became more accurate.

Other detailed methods of baggage screening incorporate Explosive Detection System (EDS) and Explosive Trace Device (ETD) technologies to detect explosives (McLay et al. 2009). Currently, EDS, first employed in the United States in 2002, incorporates tomography that simplifies the detection of risky items (i.e., explosives) by generating topographic images ("slices") from images taken from the interior of baggage (McLay et al. 2009). Similar to computer-aided smart x-ray, tomography employs a warning system to alert security personnel to any potential

problem area located within baggage. ETD, on the other hand, is used to detect whether there are explosives in baggage by way of chemical analysis (Ergün et al. 2017).

In respect to the screening of passengers beyond metal detection processes, the security industry has developed two major types of body security scanners: one that relies upon ionizing radiation (x-rays) or non-ionized radiation (terahertz and millimeter waves) (Wetter 2013). Non-ionizing radiation has less resolution than ionized radiation, and x-rays can be absorbed by water on the body (e.g., sweating) (Wetter 2013). Notably, screening with ionizing radiation allows for higher resolution as well as the identification of objects on the body. Obviously, this has led to privacy issues regarding their usage (see Panter 2013). In the Unite States, these scanners are routinely used, yet in the worldwide security, scanners are not an approved means for screening passengers yet due to various privacy issues.

Process of Passenger Checkpoint Screening

Preliminary screening of passengers prior to a flight occurs when the initial flight is booked. Passenger names are checked against "no-fly" and selectee lists. Passenger names are checked again a "no-fly" list maintained by the Terrorist Screening Center within the FBI which contains information about known or suspected terrorists through the program *Secure Flight*. Due to the secrecy surrounding the criteria for inclusion on the lists, a passenger on the "no-fly" list will be able to purchase a ticket but will be unable to print a boarding pass. When the individual checks in for their boarding pass at the airport, they are notified in person that they are not allowed to fly (Ergün et al. 2017). Currently, it is unknown how many individuals are actually on "no-fly" lists.

Other individuals who book a ticket maybe allowed to fly, but they are unknowingly on selectee lists. This Secondary Security Screening Selectee (SSSS) security measure begins when the letters "SSSS" or "*S*" are printed on a selectee's boarding pass. Prior to individual screening, this notifies TSA during a Travel Document Check (TDC) that a person must go through a more intensive screening process or they may be denied boarding in general. Just like the selection criteria for "no-fly" lists, it is unknown what the selection criteria for a selectee entail. Notably, during a Travel Document Check (TDC), TSA inspects and compares passenger identification against boarding passes for all individuals in screening lines. The TDC security process does not check for wanted felons, as TSA's primary objective is to prevent acts of air terrorism.

During TSA screening, if a passenger is not on a "no-fly" or "selectee" list, security screening is conducted to identify if any prohibited item is located in passengers' baggage or whether airport personnel have such substances when they are in sterile areas of an airport (Salter 2007). Therefore, in airport security procedures, hand searches are required, as well as the use of various technical devices to maintain comfort and speed of service. Security systems technology is used to screen three key elements: passengers, checked baggage, and carry-on baggage.

In passenger screening areas, physical barriers funnel passengers to a security official who conduct document verification to confirm the seat allocation/ticket matches both the passenger ID and documentation. From there, passengers place carry-on baggage into x-ray screening where contraband is detected. If any irregularities are detected in a passenger's carry-on, the baggage goes through additional screening either manually or through ETD search until the suspected prohibited item is located. During this process, the passenger is not allowed to touch the bag in question. Passenger screening is similar with the usage of different technologies. Passengers walk through either a metal detector or whole-body imaging technology. If any irregularities are detected, the passenger goes through additional screening through a hand-wand or pat-down search.

As such, criminals with passenger tickets (who are not on "no-fly" or "selectee" lists) are given access to sterile areas within the airport. Often it is incorrectly assumed that passengers in sterile areas do not commit crimes requiring airport law enforcement. Yet, criminal behavior by both passengers and staff in sterile areas is a common place in airports (see Fig. 3).

Thefts from cash facilities (banks/ATMs)	Shoplifting
Robbery of individuals both in sterile areas and upon aircraft	Domestic violence
Vandalism	Identity theft
Pickpocketing	Credit card skimming
Drunk and disorderly (intoxication)	Kidnappings
Theft from supply trucks	Rapes
Prostitution	Homicides
Child abductions	Human trafficking
Drug smuggling	Property theft (baggage, vehicle theft, etc.)
Physical assaults on airline workers	Concealed weapons
Trespassing in sterile areas	Child molestations

Airport Security: Procedures in Secured Areas for TSA and Private Security, Fig. 3 Types of crimes committed in sterile areas of airports

Process of Cabin Baggage Screening

Checked baggage screening did not start in the United States until the 1980s, and 100% of check bag screening did not occur until after the passage of the Aviation and Security Act (ATSA 2001). According to Shanks and Bradley (2005), prior to 9/11, less than 5% of checked baggage were screened. Currently the most commonly used technological device for baggage screening is x-ray. Notably, ICAO airports are required to hand search 10–20% (depending on the threat level) of cabin baggage screened by x-ray by hand (International Civil Aviation Organization, 2018).

TSA has incorporated a "screening partnership program" to qualified companies, which operate under federal oversight and comply with both TSA security screening procedures and other perimeter screening regulations. This is due to cost-efficiency, practicality, access to better technologies, or because private companies are more effective than governmental regulated operations (see Grover 2016). Markedly, an investigation carried out by the Government Accountability Office revealed that undercover agents were able to sneak mock explosives/banned weapons through security checkpoints 95% of the time when TSA was responsible for access control (see Grover 2016). As such, security experts have advocated for a more pluralized security approach that incorporates more private security employees working alongside TSA governmental employees.

Hold Baggage Screening

Prior to baggage screening, airlines at baggage check-in ask a series of questions regarding the passenger's trip and their baggage. Once the baggage is checked in, the baggage goes through primary screening in a secured area of the airport through an explosive detections system (EDS) or an explosive trace detection (ETD). Baggage may also go through alternative screening including manual searches, TSA-certified K-9 bomb detection teams, and positive passenger bag match.

Notably, ICAO airports are required to screen 100% of originating and transferring hold baggage by either hand, conventional x-ray equipment, or explosive detection system (EDS) equipment. If transferred hold baggage has a validation process and continuous implementation of procedures have been established for screening at the point of origin in secured areas, then an exception can be made. If threat levels are elevated, hand searching or advanced x-ray technology must be used 10–20% (depending on the threat level) of hold baggage after initial screening (International Civil Aviation Organization 2018). Currently there is a practical trend for hold baggage to be remotely screened because operators can sit in a control room and the images of bags are allocated and distributed by a computer to

different screeners (Wetter 2013). By doing so, this reduces idle times between images and aids screeners in keeping their concentration.

Access Control and Security Within SIDA/AOA Areas

Typically, within SIDA/AOS areas, a working interaction exists between governmental and private-run operations, which incorporate various technological into a layered security module that incorporates access control tactics and strategies. These tactics and strategies in regulating access control involve a working relationship between TSA, law enforcement agencies, and private security agencies often responsible for perimeter security. From a technological standpoint, advanced surveillance incorporates identification readers, closed-circuit television (CCTV), and perimeter intrusion detection systems (PIDS).

Plainclothes Law Enforcement/Undercover Law Enforcement

ICAO calls for the law enforcement patrol of the entire airport and its surroundings and to be available to respond to incidents of unlawful interference with aircraft or airport operations (Price 2018). Often, police personnel are provided by local municipalities (For example, during my police tenure, I was assigned to Hartsfield-Jackson Atlanta International Airport via Atlanta Police. Atlanta is the world's busiest airport based on passenger traffic (50,251,962 passengers annually) (source: www.atl.com).) or in some cases through an independent airport authority police force. As airport policing requires protecting critical infrastructure, uniformed officers are responsible for responding to security violations at checkpoints, security violations on inbound aircraft, airport employee criminal infractions, vehicular traffic, and irate passengers. As such, airport police must have good customer service skills, good observation skills, community-based tactics, and the ability to distinguish the difference between an upset traveler and a person who is an actual security threat. Besides responding to and investigating crimes in both sterile and non-sterile areas (see Fig. 3), police may conduct plainclothes/undercover proactive investigations. In larger American airports, plainclothes/undercover police often aid in larger-scale investigations involving passengers/baggage alongside federal agencies (e.g., Federal Bureau of Investigations Drug Enforcement Agency; National Security Agency; United States Customs and Boarder Protection; United States Immigration and Customs Enforcement; United States Secret Service; Bureau of Alcohol, Tobacco, Firearms and Explosives; United States Marshals Service; etc.).

Close-Circuit Television (CCTV)

Arguably, there are more CCTVs per square foot in commercial airports than other public areas. Most of these cameras are aimed at security gates, security doors, transition zones between non-sterile and sterile areas, passenger gates, baggage claims, and other publically accessible spaces. Often CCTV footage is monitored alongside security/police responses when a suspicious or heightened alert occurs, assessing unattended baggage from a safe distance, surveillance for theft/human trafficking, documentation for criminal investigations, monitoring of employee controlled access gates, etc.

Airport Perimeter Security

Airside and landside security requirements require effective security that integrates physical barriers, identification and access control systems, surveillance or detection equipment, implementation of security procedures, and effective use of resources (TSA 2006). Notably, since landside facilities are not typically affected by the operation of aircraft, it typically has less stringent security requirements than airside areas. Yet, airside breaches onto airfields through perimeter security are common (see Olivier 2014). Often these breaches are accidental, yet intentional breaches often occur for the following reasons: an attempt to chase down a departing aircraft because an individual has missed their flight, to take a shortcut from one area to another without driving around the airport perimeter, or in rare cases police chases or drunk drivers driving through perimeter gates (Price 2018). In such

incidents, the airfield is essentially shut down until the hazard is no longer considered a threat to aircraft on airfields.

Notably, when it comes to airport perimeter security, the FAA, TSA, and the International Civil Aviation Organization (ICAO) all have regulations and suggested practice (see: Olivier 2014). Unlike passenger screening, private security companies often regulate perimeter security. Unarmed security officers often are responsible for perimeter security. As such, their presence, while not law enforcement in nature, is to deter criminal behavior, report suspicious behavior, report violations of airport security, and report any signs of a threat to the airport (Price 2018).

In respect to boundary barriers located in landslide areas, appropriate security boundaries serve to minimize access points. Fencing around security area boundaries often incorporate motion, tension, or other electronic sensing that are monitored by private security sectors. TSA mandates that signage must be visible to identify boundaries between secured areas (1542.201) and AOA areas (1543.203). Based on topography, often chain link fences with barbed wires are established around said perimeters. As such, fences and their monitoring by private security sectors serve as a basic link of deterrence and defense against perimeter breaches (TSA 2006). In regard to technologies, perimeter intrusion detection systems include virtual fences, fence sensor systems, infrared video surveillance systems, visual spectrum video surveillance systems, mobile detection systems, fingerprint readers, and in rare cases unmanned ground and aerial drones (Price 2018). The private security sector, often represented by the American Society of Industrial Security (ASIS), continues to develop perimeter defense technologies along with training and certification for employees who implement said security measures (Price 2018).

Conclusion

The private sector plays an import role alongside governmental agencies that are responsible for security within both sterile and non-sterile areas of airports. Private agencies provide frontline screening and security functions that are supported with the integration of governmental employed police when armed intervention is required (Price 2018). From passenger screening, baggage screening, SIDA/AOA badge credentialing, undercover major investigations to perimeter security, both private and governmental agencies work intersectionally with the overall goal to safeguard civil aviation against unlawful interference.

Cross-References

- ▶ Airport Security: Incidents that Changed Procedures
- ▶ Department of Homeland Security (DHS)
- ▶ Security Management

References

Enders, W., Sandler, T., & Cauley, J. (1990). Assessing the impact of terrorist-thwarting policies: An intervention time series approach. *Defence and Peace Economics, 2*(1), 1–18.

Ergün, N., Açıkel, B. Y., & Turhan, U. (2017). The appropriateness of today's airport security measures in safeguarding airline passengers. *Security Journal, 30*(1), 89–105.

Gabbidon, S. L., Higgins, G. E., & Nelson, M. (2012). Public support for racial profiling in airports: Results from a statewide poll. *Criminal Justice Policy Review, 23*(2), 254–269.

Grover, J. (2016). *Aviation security: Airport perimeter and access control security would benefit from risk assessment and strategy updates*. Washington, DC: United States Government Accountability Office. Accessed 22 Oct 2018.

International Civil Aviation Organization. (2018). Aviation security manual [Doc. 8973]. Montreal: ICAO.

Lum, C., Kennedy, L. W., & Sherley, A. (2006). Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research. *Journal of Experimental Criminology, 2*(4), 489–516.

McLay, L. A., Jacobson, S. H., & Nikolaev, A. G. (2009). A sequential stochastic passenger-screening problem for aviation security. *IIE Transactions, 41*(6), 575–591.

Olivier, J. (2014). Airport perimeter security: Finding the right fit for your airport. *Airport Magazine*, *26*(4), 10–12.

Panter, H. (2013). Backscatter imaging and counterterrorism: An analysis of legal and privacy issues. *NSU International Journal of Criminal Justice, VIII*, 8–14.

Price, J. (2018). The role of the private sector for air transport security. In J. Szyliowicz & L. Zamparini (Eds.), *Air transport security: Issues, challenges and national policies* (pp. 63–84). Cheltenham: Edward Elgar.
Price, J., & Forrest, J. (2016). *Practical aviation security: Predicting and preventing future threats*. Oxford: Butterworth-Heinemann.
Rabkin, N. J., Berrick, C. A., & Keisling, C. (2004). *Aviation security: Further steps needed to strengthen the security of commercial airport perimeters and access control. Report to congressional requesters*. GAO-04-728. Washington, DC: United States General Accounting Office. Available at http://www.gao.gov/new.items/d04728.pdf. Last accessed September 2018.
Salter, M. B. (2007). SeMS and sensibility: Security management systems and the management of risk in the Canadian Air Transport Security Authority. *Journal of Air Transport Management, 13*(6), 389–398.
Shanks, N. E., & Bradley, A. L. (2005). *Handbook of checked baggage screening: Advanced airport security operation*. New York: Wiley.
Transportation Security Administration (TSA). (2006). *Recommended security guidelines for airport planning, design and construction*. Washington, DC: US Department of Justice.
US Congress. (2001). Aviation and Transportation Security Act (ATSA) Public Law 107-71. 107th congress, 1st session.
Wetter, O. E. (2013). Imaging in airport security: Past, present, future, and the link to forensic and clinical radiology. *Journal of Forensic Radiology and Imaging, 1*(4), 152–160.

Further Reading

Benny, D. (2013). *General aviation security aircraft, hangars, fixed-base operations, flight schools, and airports*. Boca Raton: CRC Press.
Price, J., & Forrest, J. (2016). *Practical aviation security: Predicting and preventing future threats*. Oxford: Butterworth-Heinemann.
Rabkin, N. J., Berrick, C. A., & Keisling, C. (2004). *Aviation security: Further steps needed to strengthen the security of commercial airport perimeters and access control. Report to congressional requesters*. GAO-04-728. Washington, DC: United States General Accounting Office. Available at http://www.gao.gov/new.items/d04728.pdf. Last accessed September 2018.
Szyliowicz, J., & Zamparini, L. (2018). *Air transport security: Issues, challenges and national policies*. Cheltenham: Edward Elgar.
United States, Government Accountability Office. (2004). Aviation security: Preliminary observations on TSA's progress to allow airports to use private passenger and baggage screening services: Report to the Chairman, subcommittee on aviation, committee on transportation and infrastructure, house of representatives. U.S. Government Accountability Office.

American Society for Industrial Security (ASIS)

Robert McCrie
Department of Security, Fire and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA

Keywords
Security organization · Globalization · Networking

Definition

Organizations serve numerous purposes: sharing of views and knowledge among members and supporters, standards setting, and numerous other services. ASIS International has been termed "foremost" among several industry organizations and associations concerned with protective assets from loss (Lipson 1975, p. 186). Now a global entity ASIS International faces existential issues concerning how it will serve future members.

Introduction

During World War II, the United States and the Union of Soviet Socialist Republics were allies against the Axis powers. But following peace in 1945, the two nations' political and economic systems diverged sharply with each superpower believing the other was dedicated to world conquest. The Cold War was born with the failure of the two former allies to agree on restructuring governments and territories mostly of Eastern Europe.

Hostilities between the two forces never led into a shooting conflict. Yet, elsewhere in the globe, the two economic and military powers saw "proxy" conflicts such as East and West Germany, North and South Vietnam, and North and South Korea. By the early 1950s, chances of a renewed conflict between the United States and

the USSR seemed depressingly almost inevitable, and such hostilities this time would involve nuclear arms with harm capable of reaching an unimagined level. Military and intelligence activities and investments were at high levels. Private security businesses were expanding, and a sector of private industry was inextricably responsible to produce what was needed for national security.

Individuals heading security programs in industries serving classified activities of the federal government were required to obtain security clearances in order to work on confidential projects. Furthermore, all employees who protected private information of national importance were also required to obtain security clearances or were barred from being on the worksite. "Proper clearances were a *sine qua non* to obtaining government contracts," wrote an industry historian (Lipson 1975, p. 44). These vetted organizations provided hardware, systems, and services to government and were bound to the same classified standards as were the secrecy-bound government departments and agencies. This military intelligence requirement set the basis for a trade and professional group that would support leadership in protecting people, property, intellectual property, and opportunity.

The Early Years of ASIS

Security specialists, often with military, law enforcement, and intelligence backgrounds, took responsibilities for organizations that had to meet government classification requirements. In November 1953, five men met in Detroit, Michigan, to exchange views on what was then called industrial security. The group represented the public and private sectors and included Robert L. Applegate, Office of the Assistant Secretary of Defense for Manpower, Personnel, and Reserve; Eric L. Barr, General Dynamics; Eugene A. Goedgen, General Electric; Paul Hansen, Reynolds Metals Company; and Russell E. White, also General Electric (Leading the Charge 1990, p. 9). The five continued to be in touch with each other to discuss their interests. The possibility or necessity of creating a national security organization evolved, a suggestion made first by Applegate. Other security groups, often concerned with local commercial matters, already were in existence but showed no interest in linking themselves with a national association where their identity could be lost.

A Special Security Group of 21 men met the next year in Cincinnati to discuss the matter further. Hansen had drafted a prospectus for the incipient organization. He argued "Industrial security and protection has become such an important part of history and national security that it should now qualify as a profession to be so recognized and takes its place along with the other great professions" (Leading the Charge 1990, p. 10).

Two existing organizations – the Industrial Security Council of the National Industrial Conference Board (today The Conference Board) and the Security Committee of the Aircraft Industries Association – joined the temporary governing body to help organize the new society. It would accept three types of memberships: Active members were the persons most responsible for industrial security and protection functions of an organization. Associate members, presumably down the pecking order, were ineligible for active membership but performed supervisory, administrative, or professional duties concerning industrial security. Then, government personnel concerned with security matters constituted a separate membership category. Proof of employment or government service was always a requirement. Prospective student members – a new category created years later – would need to provide their current transcript or bursar's receipt and express interest in security employment in order to be admitted to membership and enjoy the benefits.

In January 1955, the American Society for Industrial Security (ASIS) was incorporated in Dover, Delaware. Its charter stated in part that its purpose was: "To encourage, promote, aid in, and effect the voluntary interchange among members of the Society, of data, information, experience, ideas, knowledge, methods, and techniques relating to the field of industrial security." The charter additionally identified the intention "to promote uniformity in industrial security, as such, and

develop matters of mutual interest to its members." Ethics and professional standards would be emphasized. Publications and education would be supported. Hansen, ASIS's chief idealist, was elected the first president (Paul Hansen 1990, p. 12).

Rapid Expansion of ASIS

Within just a few months of its founding, security decision-makers from other workplaces unaffected by Cold War preoccupations and without government contracts sought ASIS membership. After all, most managerial issues did not involve matters of government secrecy. An expanded scope of vocational concerns and skills sharing attracted the evolving cadre of security directors in offices, healthcare facilities, manufacturing businesses, retailers, transporters, academic institutions, and still other workplaces. Membership, initially open to security practitioners in the private and public sectors, was enlarged to include affiliate memberships for suppliers of security services in 1957, though such members were not permitted to hold chapter offices for several years.

During the early decades of its existence, ASIS scrutinized membership applications with care. Did the applicant truly have a connection and commitment to protection of assets? Did any question arise about the loyalty of the prospective member to the interests of the United States or, as membership became more international, the ethos of the West? This vetting process and member services required a headquarters, and a logical place for it to be located was Washington, DC. ASIS would be governed by a Board of Directors who would henceforth set policies and institutional direction. The Board would also appoint someone to handle ongoing operations.

The first executive director served only 6 months in 1958. Next (1959–1964) came Brig. Gen. William Fagg (USAF Ret.). William D. Wright assumed leadership as a dip in membership was encountered and reversed it almost by double during his tenure (1964–1972). He was succeeded by O.P. Norton (1972–1977) during which time membership again doubled and emphasis on security education increased. (The O.P. Norton Information Resources Center (IRC) – a combination library, member service function, and archive – was named in his honor.) E.J. Criscuoli Jr. (1977–1993), security manager for General Electric's Valley Forge Space Center, led the organization in robust further expansion. His tenure included the purchase of land and the construction of a commodious headquarters building in Alexandria, Virginia, which opened in 1998. For the next executive director, the Board decided to retain the services of an experienced trade association executive, Michael J. Stack (1993–2015), instead of turning to an industry practitioner as in the past to manage operations. Expansion had occurred globally, and services became complex with membership peaking at a reported 38,000. The next year Peter J. O'Neil, also an organizational manager, became executive vice president and staff director.

Chapter Activity

From its earliest existence, emphasis was placed on the importance of active individual chapters where activities would be centered throughout the year. Chapters drove membership growth through vigorous networking and valuable local programs. Prominent leaders of the security community, not surprisingly, became chapter chairs. While initially affiliate members could not hold leadership roles, this rule was changed to the benefit of security products and service providers. (These business persons became financial supporters of chapters' activities.) Typically, chapters would meet monthly in season with a speaker on a topic of interest to the membership. The chapters often would publish their own newsletter, liaise with law enforcement and related agencies, support local security-related education, and sometimes hold their own annual seminar.

But a coming together for an annual national meeting was an early decision. The first annual Seminar in 1956 drew 254 charter members; by 2 years later membership had reached 2000 (Davidson 2004, p. 2). The Seminar was renamed the Annual Seminar and Exhibits to emphasize the

growing trade show activities and is now called the Global Security Exchange (GSX). The event spans over almost a week and combines education, technical exhibits, commercial displays, and society business. For many security leaders, attending this event is the highlight of their year in a vocational sense. Increasingly over time commercial exhibitors also used the meeting to announce and promote their latest offerings. Eleven corporations exhibited at the first seminar; in recent years over a thousand are registered.

A quarterly magazine, *Industrial Security*, was launched in 1957 as a member benefit. Over the years it became bimonthly and then monthly and was renamed *Security Management*. Meanwhile, from a fledgling start, chapters expanded to over 240 (103 international). Regional vice presidents, themselves usually former chapter leaders, would coordinate activities of chapters in their geographic regions.

Nonprofit Foundation

In its search for professionalism, ASIS established a nonprofit Foundation in 1969 to support education and research in the field. Its first major project was a survey of security executives identifying their reporting patterns and work backgrounds (Kakalik and Wildhorn 1974, p. 75). It identified that in larger firms, the principal background of a security executive was in business, followed by law enforcement and military. Another endeavor of the Foundation resulted in the founding of a vetted research quarterly, *Security Journal*, begun in 1989. (The Journal remains important in the field but is not published by ASIS.) Charles H. Davidson, IV, Foundation staff director from 1985 to 2001, argued in the first issue that security management was "a new discipline" and deserved to be regarded as "a stand-alone" management science (Davidson 1989, p. 3).

The Foundation periodically sponsored conferences that brought together leading security practitioners and security educators to share with each other what they knew and what was still needed to be done. Years later research grants were awarded on a competitive basis to scholars who would produce a monograph on a topic of importance to the membership. These would be published and disseminated as CRISP (Connecting Research in Security to Practice) Reports, available to the membership and wider community.

The Foundation also listed an early duty: "To purchase all relevant book titles in English and in selected foreign languages, to catalog, abstract, and store them at the Foundation's headquarters, and to finance or assist in financing of distribution of such abstracts to interested persons" (Poised for Greatness 1990, p. 86). These began to fill the shelves of the O.P. Norton IRC and a vast security book, film, and research report global lending library began service in 1984, soon under the longtime leadership of Eva Giercuszkiewicz.

Certifications

From its inception, the security industry was developing a "body of knowledge," once collected by James D. Calder, the University of Texas at San Antonio, in a database at the behest of the Foundation. Knowledge of results from vetted research, best practices know-how, and formal standards were becoming expectations of competent practitioners, as was the need to establish criteria for experience and examination.

Recognizing such learning and competence for security practitioners would occur through certifications. The concept, nurtured over 15 years to fulfillment by Timothy J. Walsh and others, led to the creation of a process to "recognize achievement and encourage practitioners to expand their knowledge" (The Mark of Professionalism 1990, p. 97). This decision led to the establishment of formal certification.

The Society created an independent Professional Certification Board (PCB) that painstakingly created, with outside assistance, protocols for exam admission and an examination which, when passed, would lead to a designation as a Certified Protection Professional (CPP). The first examination was in September 1978 (The Mark of Professionalism 1990, p. 98; Criscuoli 1988, p. 98). About 1000 early designees were "grandfathered in" at the commencement, based on their years of demonstrated experience as security practitioners; a few others opted to sit for the exam despite their experience.

As the examinations became required and regularized, just being allowed the opportunity to sit for the examination represented a challenge for some. Applicants needed to provide their credentials. Probity among those designated as certified was emphasized by a CPP Code of Professional Responsibility adopted in 1975.

Two other certifications were introduced in 2003, to recognize qualified security personnel with demonstrated proficiency and advanced technical knowledge. The Professional Certified Investigator (PCI) recognizes expertise in evidence collection and case preparation. The Physical Security Professional (PSP) identifies the capacity of a practitioner to conduct threat surveys, assure knowledge of security products and technology, and design integrated security systems. All PCB-developed certifications required a commitment to ongoing learning and professional development with verified recertification required every 3 years.

Further Developments

Security activities cut across a broad range of commercial, industrial, institutional, and governmental endeavors. Everything from A to Y (academic programs to young professionals) has security concerns that are particular to them while also sharing general issues with all security endeavors. Beginning as committees, 34 ASIS Councils have been created to bring specialists together sharing their common concerns, to sponsor programs for the annual seminar, and to serve as media contacts. A Chief Security Officer (CSO) Center Advisory Council was created with the goal to link interests of practitioners of large organizations.

When ASIS was in its early years, few managerial vocations were more male dominated than security. But times changed and women began assuming leadership roles. As law enforcement organizations began drawing, if not welcoming, women into their ranks, the same thing was happening in security. With women composing a significant factor of workplace personnel, it was a natural evolution for security programs to employ females as employees, managers, and executives. This notion came to be reflected at ASIS including at the senior level. The first female president of ASIS was Darlene Sherwood, 1985, and then Mary S. Rawle, 1992. They were followed by others: Cynthia P. Conlon, Bonnie S. Michelman, and Shirley A. Pierini. Moreover, women have served as past presidents of the PCB and ASIS International Foundation.

Early in its history, the original name became problematic, and a new name and focus were needed. It was no longer just *American*, as chapters all over the world were operating (currently 108 international chapters). The first ASIS security symposium was held in Brussels, Belgium, and Paris, France, in 1973. Then the word *Society* was an encumbrance for organization that thought of itself more as a professional group. Finally, *Industrial Security* spoke of a time when "plant security" for organizations churning out classified products and systems was the basis of the young ASIS. In 2002, the name was officially changed to ASIS International. A new logo was approved by the ASIS Board of Directors reflecting the way ahead: "Advancing Security Worldwide."

ASIS International: Quo Vadis?

Regardless of relevance, organizations have to be run effectively, especially so in a vocational activity some referred to as a "management science." Yet, throughout its history, ASIS has periodically experienced budget shortfalls. "We were broke," said Dennis Chesshir, president for the 1975–1976 term. He recalled "talk about dissolving the Society" despite a growing membership, a vigorous Annual Seminar and Exhibits, and 20 years' operating experience (Davidson 1989, p. 82). From 1970 to 1979, revenues grew six times, but expenses sometimes were greater. The decade of the 1980s saw more than a triple of revenues with expenses, fortunately, always a bit less. By the end of the next decade, membership topped 30,000 with positive financial net most years to create some reserves. Seminar revenues far outpaced the importance of other income streams: publishing, membership fees, educational charges, publishing and merchandise revenues, and certification fees.

At the annual meeting of 2015, ASIS President Dave N. Tyson, retiring from the hectic annual 1-year term of leadership, reported that the

organization was strong on all levels. "Today, I celebrate not only our 60 years, but also our exciting future," he exclaimed (Exceptional ASIS Members 2015, p. ?). But earlier financial reports, unknown to the vast number of members, told a different story, one of a budget out of balance. In 2013, IRS filings revealed a budget deficit of $1.6 million – up almost ten times over the previous year – on total revenues of $29.3 million. [That year 99 individuals were employed at headquarters – national and chapter officers are not paid – while the reported compensation of the top seven amounted to $2.2 million.]

Conclusion

ASIS International would have to limp before it could walk again. The Board responded with alarm by cutting historic services. Numerous employees and their positions were jettisoned with replacements in some cases of new individuals without industry experience. The ASIS Foundation stopped activities with only the name being retained. The IRC was closed with books and other materials, assembled over decades, being boxed for an uncertain future. The ASIS headquarters building that had grown enormously in value was put up for sale. ASIS International surely has a future, diminished on the national level, but remaining vigorous within many chapters. A strong national organization is needed to advance public-private cooperation, security standards, and goals, support ethics, and interact with legislative issues that impact protection activities.

Cross-References

- ▶ Security Guards: Authority and Power
- ▶ Security Management

References

Criscuoli, E. J., Jr. (1988). The time has come to acknowledge security as a profession. *Annals of the American Academy of Political and Social Science, 498*, 98–107.

Davidson, C. H. (1989). Toward a new discipline of security management: The need for security management to stand alone as a management science. *Security Journal, 1*(1), 3–13.

Davidson, M. A. (2004). *The gold standard: ASIS celebrates 50 years of advancing security.* Alexandria: ASIS International.

Exceptional ASIS Members. (2015). Exceptional ASIS members honored at luncheon. https://sm.asisonline.org/Pages/Exceptional-Asis-Members-Honored. Accessed 29 Sept 2015.

Hansen, P. (1990). The society's first president. *Security Management*, Suppl, 12.

Kakalik, J. S., & Wildhorn, S. (1974). *The private police industry: Its nature and extent. Vol. II; R-870/DOJ.* Washington, DC: U.S. Government Printing Office.

Leading the Charge. (1990). Key people and decisions. *Security Management*, Suppl, 9–22.

Lipson, M. (1975). *On guard: The business of private security.* New York: Quadrangle/The New York Times Book Co.

Poised for Greatness. (1990). *Security Management*, Suppl, 85–90.

The Mark of Professionalism. (1990). *Security Management*, Suppl, 97–104.

Further Reading

Davidson, M. A. (2004). *The gold standard: ASIS celebrates 50 years of advancing security.* Alexandria: ASIS International. www.asisonline.org.

National Advisory Committee on Criminal Justice Standards and Goals. (1976). *Report of the Task Force on Private Security.* Washington, DC: U.S. Government Printing Office.

Arrest

Halil Akbas
Troy University, Troy, AL, USA

Keywords

Power of arrest · Seizure · False arrests · Private arrests · Probable cause · Reasonable suspicion

Definition

Although there is no consensus over the definition of arrest, the US common law draws that arrest takes place when a legally authorized person, such

as the police, private security, or citizen, puts an individual under custody, especially because of his/her involvement in a crime.

Introduction

In criminal justice, arrest is an important outcome since it produces serious consequences on people's liberty and the criminal justice process. Arrestees, in many instances, are subject to searches on their persons and immediate surroundings. Arrest policies and how they are performed are highly associated with the level of the correctional population (Bittner 1967; Engel et al. 2017). For example, mandatory arrest policies for domestic violence are expected to increase the jail or prison population of this crime. Also, arrest decisions, when they are false or unlawful, can lead to wrongful imprisonments, as well as civil cases and criminal charges against responsible parties. As some research findings show, only a smaller number of arrestees are transferred to courts from the police, and only a minor portion of them ends up with incarceration. This finding indicates how the number of false arrests in the United States could potentially be high. The power of arrest is predominantly attached to law enforcement agencies, particularly to the local police; however, private security officials and citizens have also authority to make arrests under certain circumstances. This entry examines the definitional issues of the arrest, the power of arrest carried out by the public police and private security, and the circumstances under which arrest decisions are lawful/unlawful.

The Fourth Amendment, Seizure, and Arrest

A considerable number of scholars have been using the police arrest outcome as a major variable of interest in their studies, particularly to explore explanatory factors in police discretion, behavior, and decision-making process. On the other hand, there are still debates that hover around the definition of arrest. Studies emphasize the ambiguous aspects of arrests, such as the timing and conditions (when and how it starts). A major explanation for this ambiguity and complexity is that there is no unique definition of arrest (Center for Police Research and Policy 2018). First, the word arrest is never seen in the Fourth Amendment of the US Constitution. Second, the Supreme Court does not provide an exact definition of arrest.

The Fourth Amendment, whose main purpose is to protect citizens from "unreasonable searches and seizures" of government officials, uses the word "seizure." On the other hand, the seizure has a broader meaning than arrest. Law enforcement seizures can involve both properties and individuals. For example, upon a successful search, law enforcement officers can seize stolen cell phones as well as the owner of the house for keeping these stolen materials.

Under the Fourth Amendment, seizure takes place when law enforcement officers willfully infringe restraints on a person via using force or showing their authority. Restraint can be measured as the level of perception of a rational person in that she or he should not abandon the scene because of the officer's presence (Worral and Schmalleger 2018). In this context, the major question for a person's seizure is whether a rational person perceives that he/she is free to abandon the scene when a police officer stops him/her. If the person does not feel that he/she is free to leave the scene, there is a situation of a seizure.

On the other hand, a person's seizure and arrest do not carry the same meaning, that is, every arrest is a seizure, but the reverse is not true. For example, police stops – even though only less portion of them end up with arrest – would be considered seizure but not arrest. The restraint level of people's seizure is changeable; some are less intrusive and take less time compared to others. In this perspective, based on the literature, people's seizure can be examined under two categories: stops and arrests. To better understand the power of arrest, it is necessary to have a close look at the legal infrastructure of the two concepts and how they differ from each other.

Stops and Arrests

Within the context of the Fourth Amendment, stops can be defined as a concise restraint of a suspected person for a crime. However, arrest requires "a detention exceeding the dimensions

of permissible stop" (Clancy 2003, p. 129). Stops are, compared to arrests, less intrusive and take a shorter time than arrests and end up with less serious consequence for the subject. Although the difference between the two appears easy to understand, there is a tiny line between them in terms of when a stop is to be assumed an arrest or vice versa.

The common law in the United States has played a prominent role in constructing the legal definition of arrest for several centuries. However, the variable nature of the common law across jurisdictions has led to a flexible legal definition. Despite this flexibility, two prominent components of arrest can be drawn from the common law: (1) custody of the suspect, and (2) intent of the officer (Clancy 2003). Detention refers to putting the suspect under custody that starts with two conditions. First, it starts upon the law enforcement officer touching the subject. This gives a clear message to the subject that he/she cannot abandon the scene. This is, in fact, a manifestation of the officer's intent that the suspect is under custody. Second, custody may also be initiated when the subject submits to the officer's order. The second component is the officers' intent to arrest. From this perspective, arrest is not a random activity by law enforcement officers. An officer's actions to take the person under custody should be intentional. Officer's intent to arrest a person might manifest itself in certain forms such as providing a notice to him/her that he/she is under arrest or physically touching the suspect.

Legal Justification

According to the Fourth Amendment, law enforcement officers should have a justification to carry out searches or seizures. Justification is simply a suspicion. The degree of suspicion depends on the level of intrusion that the law enforcement agency performs. In other words, the law enforcement agency needs to show a stronger justification when performing a higher-level intrusion on citizen freedoms. In this case, there are two types of justification for people's seizures, each of which corresponds to different intrusion levels. These are probable cause and reasonable suspicion.

The word probable cause appears in the Fourth Amendment; however, reasonable suspicion entered the literature with the Terry v. Ohio (1968) Supreme Court decision. According to the Supreme Court definition, mere suspicion is not enough for a probable cause. Probable cause is valid when "the facts and circumstances within [the officers'] knowledge and of which they [have] reasonably trustworthy information [are] sufficient to warrant a prudent man in believing that the [suspect] had committed or was committing an offense" (Worral and Schmalleger 2018, p. 170; Beck v. Ohio, 379 U.S. 89 (1964), p. 91.). In this context, it can be established that, as the more intrusive form of seizure, arrest decisions require probable cause rather than reasonable suspicion. Many probable cause examples can be proposed; for example, a police officer can arrest a person who attempts to flee from the scene or carries incriminating evidence on his/her person.

In reasonable suspicion, however, the certainty level of suspicion that the suspect committed an offense or was committing an offense does not have to be so high as the one in probable cause. In fact, the majority of daily police activities, such as traffic stops or Terry stops, do not involve such a strong police suspicion and intrusion. Worral and Schmalleger (2018) quantify the certainty level of suspicion in probable cause situations as higher than 50%, but this level in reasonable suspicion situations lies between more than 0% and lower than 50%. Based on reasonable suspicion, police officers can stop and frisk drivers and passengers but, however, cannot arrest them. It is necessary to note that the police could carry out arrests during stops and frisks, but these arrests should still be relied on the justification of probable cause.

Arrests With/Without a Warrant

As a general approach, law enforcement agencies are encouraged to perform with-warrant arrests, but this is not required since, in many situations, getting a warrant is unachievable. Under exigent circumstances, for example, when a police officer encounters a thief attempting to steal a car, an arrest warrant is not required. In addition, where the arrest takes place is also the other factor that

determines whether a warrant is required or not. The police are not required to have a warrant when making an arrest in public places upon a probable cause. However, except for certain circumstances and the owner's consent, the law does not permit law enforcement officers to enter private homes without a warrant (Worral and Schmalleger 2018).

Therefore, if arrests are to be made in private or particular places, this requires a warrant and has to meet three conditions. First, the warrant should be given by an objective judge. Second, the law enforcement officials should have a probable cause to believe that the person is involved in a crime, and third, the suspect should be sufficiently described. Only the name is enough for the description of the offender but is not necessary if the law enforcement could determine the location of the suspect. In this case, the arrest warrant is arranged on the name "Joe Doe" and should contain very specific description of the suspect (Worral and Schmalleger 2018).

Private Arrests

Both the public and private police (including citizens) can make arrests in the United States even though the strength of power to arrest that derives from the legal framework is varied. The public police receive their authority directly from the constitutional law as well as the common and statutory law. However, private arrests are not based on the constitutional law; therefore, the common and statutory laws constitute the foundation of private arrests (Nemeth 2017).

Like the public police, private citizens have a power to arrest a person (1) if they observe that the person has committed a crime and (2) if they have a reasonable belief (probable cause) that the person committed or is committing a crime. The citizen's presence during the commission of crime is required in the first condition, but not required in the second one. Also, the authority to arrest made by citizens is changeable across jurisdictions and crime types (Nemeth 2017). For example, in New York, if the offense is not a felony, a citizen can arrest the perpetrator only within the county where the crime takes place.

In this context, private security officers have the same degree of authority as ordinary citizens to arrest a suspect. The difference between them is that private sector and business owners delegate the right to protect their property to security officers in return for money. In other words, the basic function of private security officers is to shield their employer's property (see chapter ▶ "Police: Public Versus Private Policing" in this encyclopedia). In addition, private security officers and citizens, when carrying out an arrest, are largely responsible for holding the suspect and preserving the evidence until the public police arrive (Roberson and Birzer 2010; see chapter ▶ "Private Detectives" in this encyclopedia).

False Arrests

False arrest is the unlawful detention of a person in that it occurs in the absence of probable cause or court order. That is, the arrested person can only be detained because of a suspicion that he/she committed or was committing a crime. The person cannot be apprehended as a result of only a bare suspicion. While the Fourteenth Amendment gives the authority of arrest to merely law enforcement officers, according to the common and statutory law, citizens and private sector security officers can also make arrests. Therefore, in addition to the public police, private security officers and citizens are liable for false arrests. For example, false arrest cases are most commonly encountered in shoplifting cases in which store employees or security officers detain a person for stealing something. A raising question is whether private security officers are under the mandate of the Fourth of Amendment demands when arresting such a person. The Burdeau v. McDowell case indicates that private security is not under the mandate of the Fourth Amendment (Nemeth 2017). However, this does not mean that probable cause for private security/citizenry arrests is no longer valid. According to Nemeth (2017), private citizens should have to provide a strong justification for arrest decisions. For example, citizens can generally make arrests when the offense is committed in their presence, and this has to be justified. Regardless of whoever makes it, the false arrest is an issue of a civil case that allows victims to file a lawsuit to recover the damage.

Conclusion

This entry discussed the definitional and power of arrest issues based on the legal framework in the United States. Arrest decisions have been the subject of research and particularly under intense investigation since the discovery of police discretion in the 1960s. Despite the presence of much research, it can only be drawn a general framework around what constitutes arrest rather than an exact definition of it. The Fourth Amendment of the US Constitution never uses the arrest word, so scholars have been trying to explain the concept of arrest based on the common law which is varied across jurisdictions. The common law draws two major components of arrest: detention which is putting the suspect under custody and the officer's intention to arrest the subject.

Neither stops nor seizures exactly meet the definition of arrest. It can be said that arrest is meaningfully narrower than seizures but broader than stops. Law enforcement seizures involve properties as well as people, and people's seizures can also be examined as stops and arrests. Arrests are more intrusive and take longer time than stops, therefore requiring a higher level of legal justification, that is, probable cause. Probable cause is more than mere suspicion. Although the police can stop persons based on mere suspicion (reasonable suspicion), they should have a probable level of suspicion in arrest decisions.

In addition to the public police, citizens and private security officers can also make arrest under certain circumstances. From a general perspective, private sector officers have the same degree of authority to arrest as citizens. Private security arrests majorly rely on the statutory law but not the constitution; the scope of them is changeable across jurisdictions. On the other hand, whoever attempts to make an arrest has to be tied to probable cause. Otherwise, it could result in false arrest situations and end up with lawsuits against responsible parties.

Cross-References

- ▶ Police: Public Versus Private Policing
- ▶ Private Detectives

References

Bittner, E. (1967). The police on skid-row: A study of peace keeping. *American Journal of Sociology, 32*, 699–715.

Center for Police Research and Policy. (2018). Deconstructing the power of to arrest: Lessons from research. Retrieved from https://www.theiacp.org/sites/default/files/2018-08/CPRP_Deconstructing%20the%20Power%20to%20Arrest_FINAL.PDF

Clancy, T. K. (2003). What constitutes an "arrest" within the meaning of the fourth amendment. *Villanova Law Review, 48*, 129–194.

Engel, R. S., Corsaro, N., & Ozer, M. M. (2017). The impact of police on criminal justice reform. *Criminology & Public Policy, 16*(2), 375–402.

Nemeth, C. P. (2017). *Private security and the law*. Boca Raton: CRC Press.

Roberson, C., & Birzer, M. L. (2010). *Introduction to private security: Theory meets practice*. Prentice Hall.

Worral, J. L., & Schmalleger, F. (2018). *Policing*. Boston: Pearson.

Further Reading

Button, M. (2019). *Private policing*. London: Routledge.

Engel, et al. (2019). *Power to arrest: Lessons from the research*. Cham: Springer.

Fay, J. J. (2016). *Key terms and concepts for investigation: A reference for criminal, private, and military investigators*. New York/London: Routledge.

B

Big Data

Constantine (Dean) K. Christakos
Columbia University, New York, NY, USA

Keywords
Big Data

Definition

Big Data is a term used to refer to data that exceeds the capacity of traditional databases and does not easily fit into the structure of traditional databases.

Introduction

Big Data is a term used to refer to data that exceeds the capacity of traditional databases and does not easily fit into the structure of traditional databases. The need to accommodate data of this scale and nontraditional structure appeared with the advent of event streams (such as network event logs of systems with millions of users), large deployments of sensor data, archiving and indexing of the entire World Wide Web (WWW), and visual streams of high-resolution satellite data covering large areas. Such sources can easily generate terabytes (1 TB = 1000 GB) of data if not petabytes (1 PB = 1000 TB).

Using a traditional SQL-based Postgres database for comparison, Postgres version 9, had a limit of 32 TB per table. In 2008, Yahoo claimed to have the largest Postgres database in the world with a size of 2 PB. By 2009, Yahoo was claiming a modified Postgres-based datawarehouse was managing 6 PB of data (Ahuja et al. 2009). Even in this case, an individual entry in a Postgres database is limited to a size of 1 GB. Meanwhile, high-resolution, uncompressed image formats such as TIFF can approach sizes of 4 GB. This means that new architectures were needed to accommodate the rapid exponential increase in data.

Big Data Structures, Architectures, Designs, and Models

Big Data became the umbrella term for developing infrastructure that accommodates these incoming streams of large data. Furthermore, the structure of the data itself is assumed to be large, flexible, and changing avoiding many of the structural limits of traditional database tables, for example, limits on the number of columns.

Big Data transcends the traditional limits of traditional data warehouses by no longer relying on fixed columns for data and indexing data across multiple servers through distributed hash tables, allowing their size to scale.

Big Data storage architectures are distinguished by many if not all of the following features:

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

- Support for storage of unstructured data
- Support for tables with an unfixed, unset number of columns
- Distribution of large tables split into "shards"
- Replications of data or "shards" across nodes in a Big Data
- Scalable architecture to support expansion of data capacity with added servers
- Performance architecture to support fast streaming incoming data

The design of Big Data systems supports "horizontal scaling" – that is, Big Data systems can expand their storage adding additional nodes to the Big Data network, as opposed to "vertical scaling," where additional storage and power is added to existing nodes.

The horizontal scaling inherent to Big Data means that data may be spread around thousands of nodes and Big Data systems need to tolerate the possibility of node failures or node network partitioning. Acceptance of node failure also means that data must be replicated across several nodes in the network. "Partition tolerance" in Big Data systems means that data may be inconsistent or unavailable during network partition events. The tradeoff between consistency, availability, and partition tolerance is known as CAP Theorem, the concept that a distributed database system can only have two out of those three. Since Big Data systems require partition tolerance, all Big Data systems offer either consistency or availability, but not both.

Tradeoffs between consistency and available in Big Data architectures depend on whether the structure of Big Data nodes are organized in a hierarchical architecture or a flat architecture.

The distributed nature of Big Data systems allows for ease of distributed parallel computation, so technologies like MapReduce, which process and aggregate data, are easily integrated with Big Data distributed storage and computation architectures like Hadoop, which support scaling storage across many nodes and managing resources.

The data model of Big Data systems differs from traditional SQL-based Relational Database Management Systems (RDBMS) in that the schemas and data models in Big Data are not designed to optimize on reducing redundancy. Among other reasons, this is why Big Data systems are referred to as NoSQL ("Not Only SQL") databases. NoSQL schemas account for storing less structured data than RDBMS data and so there is less need and less inclination to form optimally efficient schemas. Instead, a NoSQL schema will be optimized for ingesting and querying the data, both of which can be performed quickly and can be scaled upwards easily, so reducing redundancy is not a priority.

Since schemas can be flexible, they can be published and versioned by the Big Data server. These can be timestamped values associated with a single key, so a conceptual "row" indexed by a row key will have a varying number of columns themselves keyed by timestamp to a value. Alternately, a schema can be a set of key-value pairs, indexed by an index key. Varying columns with timestamps are a feature of Cassandra, optimized for streaming data ingestion, while key-value pair schemas are a feature of MongoDB, which is optimized for document storage and indexing.

Flexibility of schemas allows easy access to data from heterogeneous Big Data systems which can be accessed via a "data lake," so that regardless of the source of data, which may be stored in any number of different architectures, organizations can access data quickly. With a unified data lake interface, an organization can support decentralized Big Data systems whose owners may have unique schema and technology needs.

Conclusion

The order of magnitude increase in the scale of data requires new database architectures for storage because traditional architectures were unable to handle that level. Scalable Big Data architectures and a rethinking of how data is stored and organized enable the ability to handle this exponential increase in volume and diversity of types of data.

Cross-References

- ▶ Criminals: Cybercriminals
- ▶ Cybersecurity: Policy
- ▶ Machine Learning

References

Ahuja, M., et al. (2009). Peta_scale Data Warehousing at Yahoo! In SIGMOD '09: Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, June 2009, pp. 855–862.

Further Reading

Buyya, R., Calheiros, R. N., & Dastjerdi, A. V. (2016). *Big data: Principles and paradigms*. Cambridge, MA: Morgan Kaufmann.

Lai, E. (2008, May 22). Size matters: Yahoo claims 2-petabyte database is world's biggest, busiest. *Computerworld*.

Biometrics

M. Nazrul Islam
Farmingdale State College, State University of New York, Farmingdale, NY, USA

Keywords

Authentication · Biometrics · Cryptography · DNA · Face · Fingerprint · Iris · Security · Steganography

Definition

Authentication: Process to verify the identity of a request to access confidential information or service. It confirms if the requester is authorized to access and if so then what the privilege is.

Biometrics: Biological characteristics of an individual that are unique to the person and don't change significantly over time and environment.

Cryptography: Process a given message to a form that an unauthorized person cannot interpret but an authorized user can retrieve the secret message.

Security: Protection of information and system from unauthorized access, modification, or destruction.

Steganography: Process to hide confidential information inside another public information, including an image.

Introduction

Biometrics is the science of measurement and statistical analysis of an individual's physical and behavioral characteristics (Das 2019). It has been observed that every human being has a set of unique biometric features, which can be utilized to identify the person. From the very beginning of human civilization, some sort of biometrics has always been used for identification and authentication purposes. The way we recognize any of our family members, friends, or colleagues involves biometric technology, where our brain is first trained with the biometric features of the person and then it compares with stored information to identify the person. With the growth of technology, biometrics has become a crucial part of authentication and recognition processes, and, therefore, almost every system in society is incorporating biometrics (Campisi 2013).

The objective of this chapter is to present the basic principle of biometric technology. Different types of biometric features will be discussed, and then applications of biometrics in different sectors will be presented. Challenges and prospects of biometric-based technologies will be investigated.

Types of Biometrics

There are two types of biometric features as stated below:

1. **Physiological characteristics**: Unique feature in the construction and components of an individual body. These are the features with which a human being is born and hence usually

cannot change, which include the following (Das 2019):
(a) Face
(b) Fingerprints
(c) Finger geometry
(d) Hand geometry
(e) Iris
(f) Retina
(g) Ear
(h) Vein
(i) Odor
(j) DNA
(k) Voice
(l) Facial thermography

2. **Behavioral characteristics**: The features that an individual develop as he/she grows up. These are also affected by the environment around the individual and include the following (Das 2019):
(a) Handwriting and signature
(b) Typing patterns and key strokes
(c) Walking gait and other gestures
(d) Speech

Figure 1 illustrates some of the biometrics used for identification and recognition purposes. Each of these biometric features has advantages and disadvantages in terms of universality, reliability, efficiency, and complexity of applications (Prabhakar et al. 2009). A comparison of different biometrics is presented in Table 1.

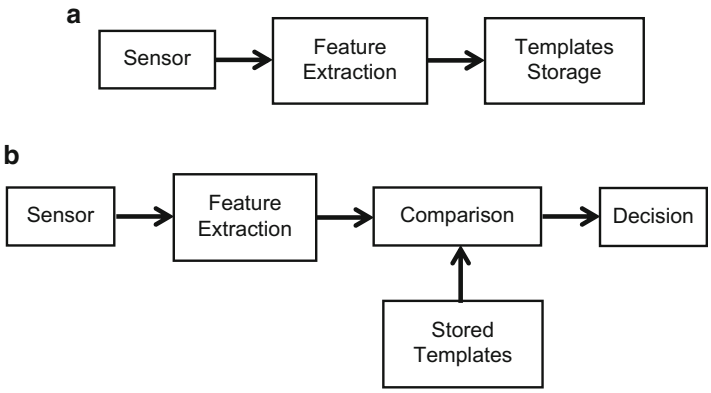
Principles of Biometric System

Biometric technology usually operates in two phases, enrollment and identification. The enrollment phase as depicted in Fig. 2a registers individuals into the biometric database. A sensor scans the individual's biometric characteristics and outputs a corresponding digital signal. Based on the biometrics, different features are then extracted and stored in the database. The identification phase illustrated in Fig. 2b also involves a biometric sensor to scan an unknown individual's biometrics, where from necessary features are extracted. They are then compared

Biometrics, Fig. 1 Different types of biometrics: (**a**) face, (**b**) fingerprint, (**c**) hand and fingerprint geometry, (**d**) iris, (**e**) retina, (**f**) ear, (**g**) vein, (**h**) DNA (Das 2019, Strickland 2012)

Biometrics, Table 1 Comparison of biometrics (Prabhakar et al. 2009)

Characteristics	Fingerprint	Face	Iris	Voice
Accuracy	High	Low	High	Medium
Ease of use	Medium	High	Medium	High
User acceptance	Low	High	Medium	High
Permeance	High	Medium	High	Low
Performance	High	Low	High	Low
Universality	Low	Low	High	Medium



Biometrics, Fig. 2 The basic principles of biometric-based technologies: (**a**) enrollment and (**b**) identification

against the features stored in the database to find a potential match.

Authentication Using Biometrics

Authentication is the process of verifying the attribute claimed to be true by an entity requesting access to a system. Usually it is the act of confirming the identity of an individual by validating the attributes presented. Reliable user authentication is crucial to individual, corporate, and state functions in order to avoid loss of confidential information, compromise of data integrity, and unavailability of service.

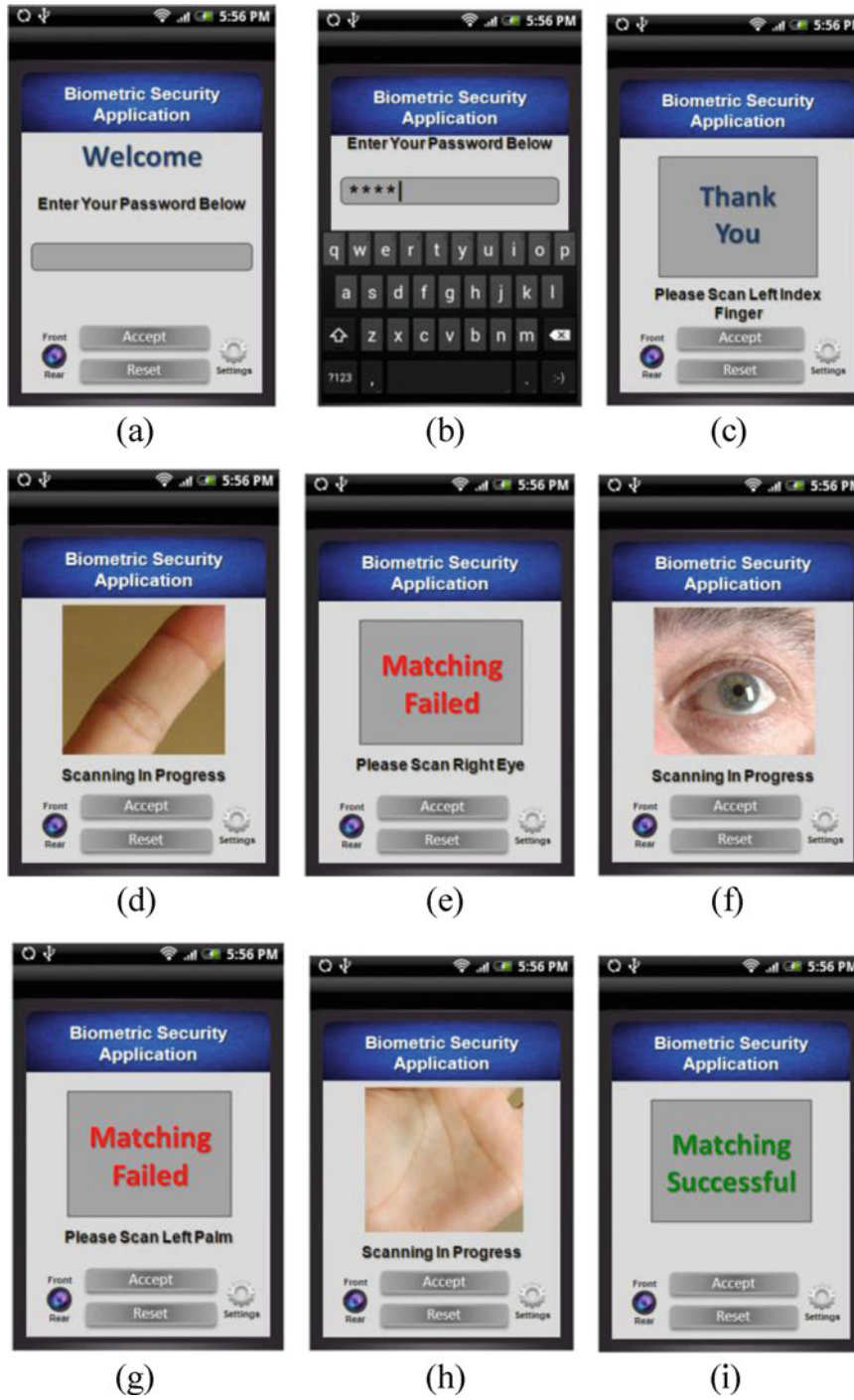
There are three factors of authentication that can be used to authenticate anyone (Stallings and Brown 2018):

(a) Knowledge: It includes something the individual knows, for example, password, pass phrase, personal identification number, challenge response, and security questions.

(b) Ownership: It involves something the individual possesses, for example, ID card, security token, and smart card.

(c) Inherence: It incorporates some unique feature of the individual that anyone inherits. Different biometrics are utilized as the key factors for authentication.

Knowledge-based authentication method suffers from individual memory, selection of poor passwords, sharing information with family or friends, and illicit acquisition by intruders. Ownership-based authentication method is becoming unreliable because of document fraud and loss. Biometric authentication has proven to be the most efficient and reliable technology (Ratha et al. 2001). The most important advantage of biometric authentication is that an individual does not have to memorize or carry anything (Campisi 2013). Recent developments in biometric technology have made the authentication process accurate, easy to implement, and very fast for automated real-time applications. As a result,



Biometrics, Fig. 3 Comprehensive authentication system developed for Android smartphone: (**a**) user is prompted for personal key such as password, (**b**) password is entered using keypad, (**c**) prompt for first biometric signature capture after successful password is provided, (**d**) first biometric signature is scanned, (**e**) feedback from the system prompting failed authentication and second try, (**f**) second signature is scanned, (**g**) feedback from the system prompting failed authentication and third try, (**h**) third signature is scanned, (**i**) successful authentication prompt (Islam 2012)

biometric authentication is becoming an increasingly important component for access to any secure facility from personal to state property.

A comprehensive authentication system can be developed to ensure the highest security and most reliable performance by incorporating different factors of authentication. Figure 3 shows an example of comprehensive authentication process developed for robust mobile computing applications (Islam and Islam 2012a).

Security of Biometrics

A great challenge with biometric-based systems is the preservation of biometric information while in storage, transmission, or processing phase (Chen and Chandran 2010). As majority of the authentication processes involve communicating with a server at a remote location either for accessing the database or sending authentication results, there is a huge vulnerability of biometric information being intercepted by intruders while in transmission. Digital encryption techniques can be applied to protect biometric information (Islam 2011). Biometric features are encrypted using a secret key and then stored or transmitted over a communication channel. An intruder cannot access encrypted biometrics for illicit use. To further enhance the security of biometrics, steganography techniques can be incorporated along with cryptography tool (Islam and Islam 2012b). Steganography is the process of hiding data inside other data which can be open to public. The most popular technique is hiding the data inside an image, where the least significant bit of the image is replaced by the corresponding biometric information bit. Figure 4 shows an example of a

Biometrics, Fig. 4 Biometric security system incorporating encryption and steganography techniques: (**a**) fingerprint, (**b**) iris, (**c**) signature, (**d**) image without any hidden information, (**e**) image with 12 hidden biometrics (Islam 2012)

biometric security system employing both cryptography and steganography. A total of 12 biometric information are used including 6 fingerprints, 3 iris, 2 personal identification, and 1 handwritten signature. They were encrypted and then hidden inside an image which demonstrates a robust and reliable security performance as shown in Fig. 4.

Challenges of Biometrics

Though biometrics offers a highly accurate and reliable authentication performance, there are a number of technical and security challenges. Some of them are listed below (Campisi 2013):

1. **User cooperation**: Biometric-based systems require individuals' cooperation in providing biometric signatures. Challenges in this regard are the following:
   (a) Uncomfortable using the devices or coming close to sensors.
   (b) Unwilling to share biometrics for storage in the system database and processing by any agency.
2. **Universality**: Receiving the same biometric signature at any time and any environment. Challenges include the following:
   (a) Some of the biometric features vary or even get distorted over time. For example, fingerprints may be less visible or recognizable, especially for working people. Handwriting changes significantly with time.
   (b) Partial biometric signature may be captured because of individual's costume or lighting condition.
3. **Processing of biometrics**: There have been a significant amount of research and development being carried out to develop efficient and fast algorithms and equipment for extracting biometric features and comparing with database templates in real time.
4. **Volume of data**: Biometric information involves a huge amount of data. Storage and transmission of such data is a great challenge.
5. **Security of biometrics**: As discussed earlier, biometrics need a high level of security.

Conclusion

Biometrics offers a great option for secure, robust, and fast authentication and identification applications. With further research and developments, biometric technologies will evolve as essential tools for almost every system in our personal and professional activities.

Cross-References

- ▶ Big Data
- ▶ Biometrics
- ▶ Data Protection
- ▶ Internet of Things
- ▶ Investigations: Use of DNA and Fingerprints
- ▶ Machine Learning

References

Campisi, P. (2013). *Security and privacy in biometrics*. London: Springer.

Chen, A., & Chandran, V. (2010). Biometric template security using higher order spectra. In *Proceedings of IEEE international conference on acoustics, speech and signal processing*, 1730–1733. IEEE, USA.

Das, R. (2019). *The science of biometrics.* Taylor & Francis.

Islam, M. N. (2011). Encryption and multiplexing of fingerprints for enhanced security. In *Proceedings of IEEE long Island systems, applications and technology conference (LISAT)*. IEEE, USA.

Islam, M. F., & Islam, M. N. (2012a). A biometrics-based security architecture for mobile computing. In *Proceedings of IEEE long Island systems, applications and technology conference (LISAT)*. IEEE, USA.

Islam, M. F., & Islam, M. N. (2012b). A secure approach for encrypting and compressing biometric information employing orthogonal code and steganography. In *SPIE Proceedings in optical pattern recognition XXIII*, volume 8398, SPIE, USA.

Prabhakar, S., Pankathi, S., & Jain, A. K. (2009). Biometric recognition: Security and privacy concerns. *IEEE Xplore*, 22–45. IEEE, USA.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614–634.

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Hoboken: Pearson.

Strickland, E. (2012). The biometric wallet. In *IEEE spectrum*. IEEE, USA.

Further Reading

Bala, D. (2008). Biometrics and information security. *Proceedings of the 5th annual conference on Information security curriculum development (InfoSecCD '08) ACM*, 64–66.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *IEEE International Conference on Computer Science and Electronics Engineering*.

Kaufman, L. M., (2009). Data security in the world cloud of computing. *IEEE Security and Privacy, 7*(4), 61–64.

Li, M., Lou, W., & Ren, K. (2010). *Data security and privacy in wireless body area networks, 17*(1), 51–58.

Border Security

Keith Cozine
College of Professional Studies, St. John's University, Queens, New York City, NY, USA

Keywords

Borders · Security · Transnational Threats · Smuggling · Trafficking · Migration · Counterterrorism · Travel documents · Passport Control · Baggage Control · Ports of Entry

Definition

Border security is the step that nations take to prevent people or items from entering and departing into their country that may pose a threat or other adverse consequences or otherwise violate that nation's laws.

Introduction

One could argue that borders have been around since humans first began to settle in fixed locations, claiming that location as their own. As humans moved from hunter-gathers to agrarian society, they began to mark land over which they believe to have exclusivity over its use. These lines of ownership or borders could exist only in one's mind, meaning that this is what this person or group of people believed to be theirs, accepted by others outside their borders, based on physical features of the earth, or barrier such as primitive fences or walls to mark their land. Today, borders most commonly thought of as the divide between political entities, usually between countries. Just like in early times, these borders could be imaginary, existing only in the mind of certain individuals, borders that are agreed upon, and demonstrated by lines on a map based on conquest, threat, agreements with others, natural physical feature, or walls and other means of marking territory. Just like early man marking their territory, borders have become a symbol of national sovereignty where that nation exerts exclusive control. Borders represent national sovereignty that need to be protected and controlled to maintain that country's sovereignty; therefore, border security is an important component of any country's national or homeland security (Phelps et al. 2014).

Throughout much of history, the primary threat to border security was military incursion from hostile neighbors or other foreign forces. In fact, just a quarter of a century ago, what Winston Churchill famously referred to as an "Iron Curtain" divided Europe between East and West. The North Atlantic Treaty Organization (NATO) was founded at least in part in response to the threat posed by the Soviet Union and Soviet expansionism. As a result, in many parts of the world, much of what would be considered border security was handled by countries' military organizations (Cozine 2016). However, the use of military power against another state may no longer be the practical option if these two opponents are both militarily and economically powerful. The cost of war can become a high one, not just in the cost of lives but also the harm done to both nations' economy, as well as the global economy.

Today's globalized world seems to continually shrink to a point where time and space are less and less important. Advancement and innovation in shipping allow for goods to be loaded onto ships, cross vast oceans, and then be unloaded and delivered to markets in days. Air travel, which not long ago was available only to the elite, is now affordable to all but the world's

poorest. This current era of globalization has been decades in the making. However, few argue with the notion that the end of the Cold War and East-West divide was a catalyst, speeding up the process and bringing its benefits to the world as a whole. Advancements in technology and transportation that facilitate more efficient and faster trade and travel have not exclusively benefited legitimate transnational actors but have has also benefited international criminals, terrorist, and their organizations (Rees 2006). With globalization and the barriers lifted by the end of the Cold War, the security threat has shifted somewhat from state-centric threats to transborder issues such as financial collapse and global warming, pandemics, and threats from a variety of non-state actors. The openness that globalization has created engenders an environment in which the illegal trade of drugs, arms, intellectual property rights, and money is booming and has allowed for terrorist organizations to operate globally as well (Cozine 2010).

Threat

The terrorist attacks of September 11, 2001, and the way that those responsible were able to gain entry to the United States quickly focused the spotlight on border security as a major national security concern. Advancements in technology and transportation that facilitate faster and more efficient trade and travel have not exclusively benefited legitimate transnational actors; they have also benefited international criminals, terrorists, and their organizations (Rees 2006). The September 11th hijackers were able to take advantages of flaws in the US border security and visa system to pass through ports of entry, in some cases, several times, to train, plan, and carry out the attacks.

The attacks and the way that those responsible were able to gain entry to the United States quickly focused the spotlight on border security as a major national security concern. In order to better understand how the September 11th attacks occurred, the US Congress passed legislation that created the National Commission on Terrorist Attacks Upon the United States, more commonly known as the 9/11 Commission. The Commission was tasked with preparing a full and complete account of the circumstances surrounding the September 11th terrorist attacks. It quickly became apparent to the Commission that the terrorists' ability to successfully gain entry to the United States was a key element in their ability to carry out the attacks. The topic of terrorist travel was deemed so important that it was covered in much greater detail in the form of a staff monograph separate from the Commission's final report (Cozine 2010).

The profile of those individuals who pose the greatest threat, at least in terms of terrorism, has evolved over the past decade and now focuses on homegrown violent extremism – a threat that arises from within a domestic population where citizens or residents embrace an extremist ideology and take violent action in furtherance of that ideology (Southers 2014). Much has been made of the concept of the lone wolves, inspired to carry out terrorist attacks on their own, without any specific direction from a terrorist organization. In reality, the most catastrophic attacks and sophisticated plots were carried out in some part by members of the domestic population that traveled to other areas of the world to receive training and direction from terrorist organizations. This is a phenomenon that first came to light in the aftermath of the July 7 bombings in London and most recently played out in Paris and Brussels (Cozine 2016). This threat environment has created a situation where border security and those organizations charged with securing a nation's borders now face the dual challenge of dealing with both homegrown and external threats. Traditional border security was focused on outsiders seeking to do harm – a concern that still exists today as highlighted by the June 2016 attacks at the Istanbul Airport that were carried out by attackers from Russia, Uzbekistan, and Kyrgyzstan who entered Turkey a month before the attack by illegally crossing its border with Syria carrying the suicide vests and bombs used in the attack (Karimi et al. 2016). However, there is also an internal threat of one's own citizens traveling overseas to Iraq or Syria to join terrorist organizations and possibly

return home to carry out attacks. Since 2011, nearly 40,000 fighters, including at least 6,900 from Western countries, have traveled to Syria. Around 250 of the Westerners traveled from the United States and 5,000 traveled from European Union countries. It is suspected that one third of the European fighters have returned home from Syria (House Homeland Security Committee 2016 June).

The reality is that terrorism is only one of the many man-made and natural transnational threats and challenges that face those tasked with securing a nation's borders. Today, illegal migration, human smuggling, drug trafficking, counterfeit goods, and mass migration are just a few of the man-made threats the border security officials must combat. Add to this mix a variety of natural threats such as pandemics or invasive species and the threat picture becomes even more complex. Adding to this complexity is the question of how border security agencies and organizations provide security while still facilitating legitimate trade and travel across international borders, a process vital to the health of the global economy. Nearly 1 million people and 67,000 cargo containers enter the United States each day (Custom and Border Protection 2016). Finding those individuals or items that pose a security threat among this avalanche of people and goods that cross the border each day is truly a daunting task. But the nature of borders and the strategies for securing them are as varied as the threats that are faced.

Nature of Borders and Border Security

Borders can take many forms: natural, such as rivers and other bodies of water; physical, such as walls and fences; agreed upon lines on a map; or any combination of these. How well border security and integrity are maintained directly affects those living within those borders and those who wish to profit from violating internationally accepted rules of national sovereignty. The characteristics of borders are often dictated by societal and political institutions within a particular country as well as their relationships with their neighbors and potential threats that lie just on the other side of that border (Cozine 2016).

Natural borders will often dictate a country's border security strategy. Geography has long been a barrier that has separated people into separate groups, and even today these mountains remain as a physical and political border separating China from Pakistan, India, and several other countries. The Alps have long served as an impressive physical border in Europe. The Alps have allowed for Switzerland to maintain independence political neutrality since 1291 and has not been in a state of war since 1812. This, despite the fact that during this time there has been a state of near constant hostility all around them, including two world wars. Bodies of water have also served an import physical barrier that separated people and established political borders. The English Channel has separated Great Britain from the European continent, thus allowing Britain to implement many policies separate from those of the European Union including maintaining border control between itself and the rest of the continent. The oceans, seas, and other large bodies of water remain formidable barriers. For proof, one needs to look farther than Australia and New Zealand, two large island nations that have never been invaded.

When natural barriers do not exist between countries and one country sees its neighbors or things within its neighbor's borders as threats, many countries feel the need to fortify borders with artificial barriers to prevent or limit unwanted incursions across the border. The most common artificial barrier between nations are walls. Walls are erected to prevent or deter an individual, groups of people, even foreign forces from crossing a nation's border or designed to funnel legal border crossings through checkpoints or ports of entry setup at specific locations. Walls are not the only type of artificial barriers used to fortify borders. Other types of barriers include fences, armed patrols, and air and marine patrols. Increasingly, technology is being implemented either in lieu of artificial barriers or to augment both artificial and natural barriers. These include measures such as motion sensors, thermal image cameras, and even unmanned aerial vehicles, all of which can be

monitored remotely by user who can dispatch a response team to deal with unwanted border incursions (Phelps et al. 2014).

Border security is not exclusive to the geographic location where one country meets another. Individuals and goods entering a country legally need to enter that country through a port of entry. Ports of entry are specific locations where individuals and goods can enter a country legally by land, sea, or air. They typically have a staff of people who check passports and visas and inspect luggage to assure that contraband is not imported and that individuals who are not eligible to enter a country or pose security risk are refused access. Ports of entry at international airports are usually divided up into two screening areas: passport control and baggage control. At passport control, it is individual people who are screened in terms of their eligibility to enter the country. Individuals are screened for things such as their citizenship, whether they have the required papers such as passport and visas if required, and whether there is something in the individual's background that would make them ineligible to enter the county such as previous immigration violations, criminal record, or a danger to the security of that country. When an individual is ineligible to enter a country, they might try to sneak past passport control and border security officials by presenting fraudulent travel documents to change their identity or other characteristics about them such as their citizenship. There are a variety of types of fraudulent documents that an individual can use to try and gain entry to the country that they would otherwise not be allowed to enter. These include counterfeit documents; documents that have been altered in some way, such as switching the photograph or name; using a document that belongs to an individual who looks similar to the traveler, a technique known as impostoring; or using a genuine document that is real but has been obtained by identity theft or some other illegal means. This means that officials at passport control must very quickly determine an individual's citizenship, whether they have the required documents, whether those documents are genuine, and whether the individual has anything in their background that would make them ineligible to enter the country. In recent years, many technological advances were introduced into the passenger screening process, including a variety of security features within the passport itself to aid in detecting counterfeits, radio-frequency chips that transmit information to border screening computer systems automatically, and increased use of biometrics such as fingerprint and facial recognition technology.

At baggage control, travelers' belongings are screened for prohibited items, such as drugs, counterfeit merchandise, agricultural and food products as well as insects which may pose a risk to a country's ecosystem, currency that needs to be reported, and items that require that a duty or other tax be paid. Screening at baggage control includes examining both the traveler and their baggage for prohibited items. Some common examples of how people try and sneak prohibited items through baggage control include hiding items in the lining or secret compartments of their luggage, making it look like other items such as prepackaged items and food products, sewing it into their clothing, simply strapping it on their body, or swallowing the drugs so that it passes through their digestive system after they have successfully entered through the port of entry. The only way for border officials to detect this type of smuggling is by the use of an X-ray machine. The reality is the way in which an individual can try and sneak prohibited items through baggage control is limited only by their imagination.

In addition to passengers and their baggage, many international airports also have large amounts of cargo pass through that all need to screen for prohibited items as well as cargo where duty needs to be collected. The same is true of seaports and ports of entry at land borders. At seaports, passengers and crew are screened for eligibility to enter the country, and cargo is inspected. What makes seaports somewhat different is the amount of cargo that comes in and out of seaports. One needs only to look at the enormous size of a modern container ship to have an idea of how much cargo passes through a seaport in a

given day. For example, the Triple E container ship has a capacity equivalent to 18,000 20-foot containers that would fill more than 30 trains, each a mile long and stacked two containers high (Kremer 2013). Many ports of entry at land borders have to deal with a high volume of both individuals seeking admission (i.e., pedestrians or individuals in vehicles) and large amounts of cargo carried by tractor trailers or freight trains. Adding to the challenges is the fact that these conveyances themselves can be used to smuggle both people and prohibited items through a port of entry. The number of places to conceal both items and people on a large container ship is near limitless. Hidden compartments in cars, trucks, and trains have all been used to smuggle people and goods across the border in the past. This sheer volume of cargo and people coming through a port of entry on any given day makes providing for effective border security while at the same time facilitating efficient trade and travel a daunting task.

When nature does not serve as a mechanism for border security, the characteristics of border security are often dictated not just by societal and political institutions within a particular country but also the relationships they have with their neighbors as well as potential threats that lie just on the other side of that border. For an example of how internal politics and a volatile relationship with one's neighbors impacts a country's border security strategy, one needs to look no further than the Korean Peninsula and the demilitarized zone (DMZ) that is between North and South Korea. The DMZ is a 2.5-mile-wide and 160-mile-long barrier created by both countries surrounding the military demarcation zone that serves as the border separating the two countries since the end of the Korean War in 1953 (Phelps et al. 2014). With both countries' militaries constantly patrolling their respective side of the DMZ while on alert for acts of aggression by the other side, the DMZ is the most heavily militarized border in the world with one side in a constant state of readiness to respond to threats from the other side (Phelps et al. 2014).

The nature of border security is not static and often changes over time. Perhaps no place in the world illustrates this better than Europe. Just a quarter of a century ago, what Winston Churchill famously referred to as an "Iron Curtain" divided Europe between East and West. Much like the border between North and South Korea, the Iron Curtain separated members of the North Atlantic Treaty Organization (NATO) on one side and Warsaw Pact members on the other. With the fall of communist regimes in Eastern Europe, it is now possible to drive from Spain to Finland without passing through a single border check. In reality, even before the fall of communism, the elimination of internal borders between democracies in Western Europe while at the same time strengthening their common external borders has been a goal in many European countries.

Since the 1970s, countries in Europe have worked together on an intergovernmental basis to combat cross-border threats such as terrorism, drug trafficking, and illegal migration. By 1980, the frequency of this cooperation was a growing recognition that the freedom of movement throughout the continent was a key element to establishing a common internal market; it became clear that this type of informal cooperation was no longer adequate to address cross-border issues faced on the continent (Direction Générale des Douanes et Droits Indirects 2015). Since EU member states could not reach an agreement on how to formally deal with these issues, France, Germany, and the Benelux nations agreed that the territory among their states would be without internal borders. This border-free zone became known as the Schengen Area, which was named after the town in Luxemburg where the agreement was signed on June 14, 1985. On June 19, 1990, the Schengen member states (Adopted by the Kingdom of Belgium, the Federal Republic of Germany, the French Republic, the Grand Duchy of Luxembourg, and the Kingdom of the Netherlands.) signed the Schengen Implementation Convention (SIC) to formalize their agreement on how the rules of the agreement's framework would be put into place. The convention called for the removal of checks at internal borders, common rules for crossing external borders, harmonization of entry and visa conditions,

enhancement of police and judicial cooperation, and the establishment of a common information technology system for border security. By September 1, 1993, all Schengen members had ratified the convention and the agreement officially entered into force. The Schengen Area became a reality in the spring of 1995 when, with only a few exceptions, border checks were eliminated between signatory nations and a single external border was created where members carried border inspections with identical procedures based on common rules for visa and entry requirements as well as asylum rights (European Union 2009).

During the 1990s, several other EU member states signed on to Schengen Agreement, and the Treaty of Amsterdam brought the Schengen Agreement and subsequent acquis (Schengen Convention; agreement accession to the Schengen Convention by Italy, Spain, Portugal, Greece, Austria, Denmark, Finland, and Sweden; the decisions of the Executive Committee and the Central Group; and Union acts adopted by the European Parliament and/or the Council after the Schengen acquis was integrated into Union law.) into the framework of the EU. When the treaty entered into force on May 1, 1999, every EU member state was within the Schengen Area with the exception of the United Kingdom, which includes England, Wales, Scotland, Northern Ireland, and Ireland. Schengen, along with the establishment of the euro as a common currency, became shining symbols of the reality of European integration. Ironically, today because of threats of terrorism, transnational crime, and mass migration stemming from conflicts in the Middle East and other regions, some Schengen members have reinstituted border checks on their borders, and there are political movements in some countries calling for withdrawal from the Schengen zone.

Border Security in the United States

For the latter half of the twentieth century, the continental United States was long thought to be insulated from a massive attack other than a Soviet nuclear barrage. These all changed on September 11, 2001, when its vulnerability was revealed. While September 11 brought this vulnerability to the forefront, a variety of non-state actors have long benefited from the ever-increasing openness and interconnectivity of the world to operate across national borders in violation of law and evading law enforcement to achieve their goals (Andreas 2003). However, the September 11 attacks did result in a dramatic restructuring of the United States' approach to both border security and intelligence. The Homeland Security Act of 2002 created the Department of Homeland Security (DHS) and, within it, Customs and Border Protection (CBP), which is the agency primarily responsible for border security in the United States at and between ports of entry.

Border security enforcement is the responsibility of three operational components within CBP: the Office of Field Operation, US Border Patrol, and Air and Marine Operations. The Office of Field Operations is primarily responsible for screening individuals and goods at air, sea, and land ports of entry. The US Border Patrol is the component whose main mission is to detect, interdict, and prevent individuals entering the United States illegally or smuggling people or contraband between official ports of entry. The Air and Marine Operations provides an air and maritime force to support the other two operational components by detecting, interdicting, and preventing the unlawful movement of people, illegal drugs, and other contraband toward or across the borders of the United States.

In addition to CBP, other agencies within DHS play an important role in border security: Immigration and Customs Enforcement (ICE), Citizenship and Immigration Services (CIS), and the US Coast Guard (USCG). Like CBP, ICE was created as part of DHS with the passage of the Homeland Security Act of 2002 and is the largest investigative organization within DHS by incorporating and consolidating the investigative elements of the former US Customs Service (USCS) and Immigration and Naturalization Service (INS) into one agency. ICE has two main operational components that carry out the daily enforcement and investigation activities—Enforcement and Removal Operations (ERO) and Homeland Security Investigations (HSI). ERO is primarily tasked

with interior enforcement of immigration laws including identifying, apprehending, detaining, and removing aliens residing illegally within the United States or other aliens deemed removable by an immigration judge. HSI is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States. CIS is responsible for overseeing lawful immigration to the United States while also maintaining the integrity of the country's immigration system. The USCG is unique in a number of ways including that it is the only component of the US Armed Forces that is not housed within the Department of Defense, but rather it is part of DHS; it simultaneously acts as a military service, a law enforcement organization, and a regulatory agency. Included among the USCG's many missions are defending the United States' maritime borders by disrupting and deterring the flow of illegal drugs and undocumented migrants at sea, and preventing their entry via maritime routes to the United States.

There are also a variety of law enforcement agencies outside of the DHS that play a role in border security intelligence. Within the Department of Justice (DOJ), there are two such organizations – the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA). The FBI is involved in investigating a wide variety of issues directly related to border security, including international terrorism, human trafficking, and organized crime. The DEA's primary mission is to investigate and prepare for the prosecution of major violators of controlled substance laws operating at interstate and international levels. The Department of State's (DOS) Diplomatic Security Service (DSS) is another law enforcement agency that is directly involved with border security. In addition to its protective mission, DSS also investigates passport and visa fraud.

Conclusion

A country's border security strategy varies greatly depending on that country's geographic location, political institutions, and social and cultural heritage. For example, the border the United States shares with the Canada is the world's longest undefended border, stretching nearly 9,000 kilometers across land and water, yet there are still ports of entry and other security measures along (Phelps et al. 2014). This is in stark contrast to the borders of countries in the European Union where there are no border checks when crossing between many member states. On the other side of the spectrum is the heavily militarized border between North and South Korea. Complicating the matter further is the fact that borders and approach to border security are not static and will often change as one country's relationship with their neighbors change and events occur in that neighboring country that directly impact the security of one's own border security.

The fact is that no country can effectively go it alone when it comes to border security. In an ever more globalized world, what happens inside your neighbors' borders impacts your own. Today, the threat to security does not just come from citizens of some far-off country that follow a particular violent ideology or make a profit by exploiting a country's laws and weaknesses in border security measures to engage in illicit trade but one's own citizens traveling overseas to carry out similar activities. Another major challenge is how a country, or groups of countries, provides border security while facilitating the efficient movement of legitimate trade and travel. For border security to be effective in confronting the diverse cross-border threats faced today, cooperation is needed not just with domestic partners with border security responsibilities but also with international partners to ensure the integrity and security of their borders and the safety of their people.

Cross-References

- ▶ Big Data
- ▶ Biometrics
- ▶ Department of Homeland Security (DHS)

▶ Maritime Security: Contraband
▶ Terrorism: International

References

Andreas, P. (2003). Redrawing the line: Borders and security in the twenty-first century. *International Security, 28*(2), 78–111. https://doi.org/10.1162/016228803322761973.

Cozine, K. (2010). *Transgovernmental networks as a tool to combat terrorism: How ICE attachés operate overseas to combat terrorist travel*. Doctoral dissertation, Rutgers The State University of New Jersey-Newark.

Cozine, K. (2016). Fragmentation and interdependency: Border security intelligence in North America and Europe. *The International Journal of Intelligence, Security, and Public Affairs, 18*(3), 175–197.

Custom and Border Protection. (2016). On a typical day, About CBP. Retrieved from https://www.cbp.gov/about

Direction Générale des Douanes et Droits Indirects. (2015). La direction nationale du renseignement et des enquêtes douanières. Retrieved from http://www.douane.gouv.fr/articles/a12574-la-direction-nationale-du-renseignement-et-des-enquetes-douanieres

European Union. (2009). The Schengen area and cooperation. European Union. Retrieved from http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm

House Homeland Security Committee. (2016, June). The ISIS terror threat in America. *Terror Threat Snapshot*. Retrieved from https://homeland.house.gov/wp-content/uploads/2016/06/Terror-Threat-Snapshot-June.pdf

Karimi, F., Almasy, S., & Tuysuz, G. (2016 July 1). ISIS leadership involved in Istanbul attack planning, Turkish source says. *CNN*. Retrieved from http://edition.cnn.com/2016/06/30/europe/turkey-istanbul-ataturk-airport-attack/

Kremer, W. (2013, February 19) How much bigger can container ships get? *BBC News*. Retrieved from https://www.bbc.com/news/magazine-21432226

Phelps, J., Dailey, J., & Koenigsberg, M. (2014). *Border security*. Durham: Carolina Academic Press.

Rees, W. (2006). *Transatlantic-counterterrorism cooperation: The new imperative*. London: Routledge.

Southers, E. (2014). *Homegrown violent extremism*. New York: Routledge.

Further Reading

Andreas, P., & Biersteker, T. J. (2014). *The rebordering of North America: Integration and exclusion in a new security context*. New York: Routledge.

Koslowski, R. (Ed.). (2011). *Global mobility regimes*. New York: Palgrave MacMiollan.

Bribery

Kenneth J. Grossberger
John Jay College of Criminal Justice, New York, NY, USA

Keywords
Bribe · Criminal · Moral security

Definition

Bribery infers an "illicit exchange" in which a person or company offers a government or public official, officer, or employee valuable items, such as gifts, money, property, etc., in return for contracts, services, or other treatment (Noonan 1984).

Introduction

Bribery is often deemed illegal by society, ethically unacceptable, and judged as morally questionable due to the harm that it causes (D'Andrade 1985; Green 2005; Horder 2011; Noonan 1984). The premise of this offense is that ". . .accepting a bribe involves the violation of an implicit or explicit promise or understanding associated with one's office or role and that, therefore, accepting a bribe is always prima facie wrong" (Carson 1987, p.). Laws against bribery, that is, making bribes illegal, are tied to moral or ethical violations caused by the bribe act itself, namely, corruption. Consider the comparison of offering a free car to a politician versus a private business owner in exchange for hiring your nephew. The act is the same, but the former would be defined legally as a bribe as it violates the fair process of selecting employees for public positions; there is no similar requirement for a business owner. There are other people, due to the capacity in which they serve, such as private security guards, loss prevention employees, fire and emergency personnel, and public law enforcement to name a few, who may be offered bribes because they hold power over others, such as arsonists or criminals.

For example, a shoplifter may offer a bribe to the retail loss prevention employee who apprehended her in order to avoid arrest and prosecution. Security managers, as well as their employees, may be tempted by bribes. For instance, security personnel may be bribed to allow employees or even criminals to enter a premise to steal, or private security prison guards may accept bribes from their prisoners in exchange for a variety of privileges. Private security investigators may be bribed to not report their findings of negligence (e.g., collapsed structure or building), arson, ineptitude, etc. This entry provides an overview of the practical, legal, and moral dimensions of bribery in the context of protective security professionals and security guards.

The Cultural Aspects of Bribery

Noonan (1984) stated that while a lack of admission was common, and the deceit inherent, the behavior was pervasive as it occurred in almost every society and in every era. Yet despite its negative connotations, bribery has been rationalized in the following ways:

1. "Everybody does it." Noonan has shown bribery occurred in numerous eras and societies indicating the pervasiveness of illicit exchanges.
2. "It is necessary to do it." This reasoning implies it was done for job survival or to gain acceptance in a given situation.
3. "Reciprocities are formally indistinguishable." This argument relies on a slippery slope premise in that many types of bribery seemed to be non-corrupt exchanges.
4. "It is immorally enforced." Noonan referred to the inconsistencies inherent in the hypocritical ways the rules against bribery were only sometimes enforced or where bribery was situationally or cultural mandated. For example, if it was routine that employees steal goods from a warehouse, and the security guard is invited to join in, then the guard is corrupted and the behavior is reinforced.
5. "The material effect . . .is either trivial or undemonstrated." This argument essentially suggests that no real harm is done and that bribery in many cases amounts to no more than a societal "taboo." This moral logic is the same as arguing that pilfering really is not stealing and is a victimless crime (such small-scale shoplifting in retail stores, especially when the loss prevention security guard looks the other way in return for some of the stolen goods).

Noonan (1984) contended that, whatever the rationalization, the future of the bribe remains problematic, because, despite the level of relative unacceptability, the act itself is "universally shameful," is a "betrayal of trust," and contravenes a "divine paradigm." He stated that "bribery is a legal concept," thus, the punishment comes from the law, but enforceability is an issue and enforcement of the law remains selective in that the proscription of such illegal reciprocity depends on accepted cultural norms and contextual notions. While bribery itself is "criminal and consensual," the motivations are often dissonant and personal.

Bribery, Security Personnel, and Insurance

Security personnel protect residences, commercial office buildings, institutions (schools, hospitals, nursing homes), government buildings, retail stores, warehouses, and airports, to name a few. Security guards may be bribed for access to such premises (when the officer's post responsibility is access control), to look the other way when someone engages in wrongdoing, and to abet theft. Payments can be in cash, a share of the stolen merchandise, or sex, favors, or food. A key factor is that security guards are typically low paid, which makes them vulnerable, and thus the risk is enhanced. The act of bribery is usually considered a crime (see ► "Investigations: Criminal"), based on criminal justice theory, which states that a crime has three elements: the mens rea (criminal

intent; intent to coerce decision or action), the actus reus (the criminal act itself, offering or taking of something of value in exchange for bribed acting, promising to act within his/her capacity or duties to provide briber with a benefit, including going unpunished for breaking the law), and the facts of the case (Stein 2012).

Security guards may be natural targets for bribes (see ▶ "Retail Security: Use of Security Guards"). For example, can private security guards legally perform searches? There are different rules for searches in the private sector. Security guards cannot use "reasonable suspicion" as a cause for a search as that is the province of law enforcement under the US Supreme Court ruling in *Terry v. Ohio* (Cornell Law School n.d.). Security guards must have probable cause (a high standard of evidence) to make a stop, which means the security guard must see the act (see ▶ "Retail Security: Use of Security Guards"). However, in retail, for example, a security guard working loss prevention in stores may check a shopper's bags, if it is a store policy to do so (and the guard's post orders permit it), but then only with the permission of the shopper. But if the guard sees the shopper take something, and then try to leave, the officer may stop the shopper and call the police.

This is a classic opportunity for a shoplifter to offer a guard something in return for being released. The guard's training should take effect, and if not, then the potential for a bribe will increase. If the guard stops the shopper (or takes him/her into custody), then the guard might be accused of illegal restraint. As security guards are not police officers, they are not protected by various "shield" laws which insulate police personally from civil suit. Under citizen's arrest laws, the guard may make the stop but must be sure or may be subject to arrest and lawsuit herself. Thus, a security guard, like any other citizen, may arrest another person without a warrant but subject to certain limitations (Wollan 2016).

Security guard companies typically have general liability insurance, which provides protection against most causes of action involving physical security (see ▶ "Security: Contract"). Many companies also have Employers Practices Liability Insurance (EPLI) which protects companies from so-called third-party actions or discrimination cases. If a private undercover agent or a store detective is accused of bribery, the defendant's lawyer might threaten a third-party action to induce the company to drop any criminal charges. Lawsuits that result therefrom can be costly. Security companies may buy crime bonds, which protect companies against such events as employee dishonesty and "mysterious disappearance," where items are missing without explanation while guards are on duty. Many such cases are the results of the guard being bribed to assist in the theft. General liability, third-party insurance, bonds, and other forms of protection can be expensive and are major concern in private industry. Most lawsuits are settled prior to trial, but the effect on the defendant company's loss run (the record of losses in an insurance policy) can prove to be quite expensive. The legal and reputational damage to the security guard may be serious and result in banishment from the security industry in that jurisdiction.

Security guards perform basic functions: observe and report, and post and patrol. Thus, they are responsible for basic security (perimeter patrol, access control, protection of assets, and reporting theft and dangerous conditions). But corrupt officers endanger the very people and assets they are hired to protect. This is especially so for critical assets in such facilities as hospitals, nuclear power plants, banks, homeless shelters, museums, law offices, and government offices. Corrupt guards that fail to protect these assets and the people therein, by accepting bribes do not do their jobs, violate the basic precepts of their position, invert their purpose, and abuse the trust given to them. The potential damage done by a security guard who accepts a bribe to allow access by the wrong people, allows theft and vandalism, and looks the other way when crimes are committed, or partakes in such crime, could be severe or even catastrophic. Thus, the risk posed by the bribery of a security officer ranges to the extreme and is a highly significant issue for the industry.

The Morality of Bribery

D'Andrade (1985) declared flatly that "bribery is wrong" and is "immoral almost by definition in the same way that murder is." However, Horder (2011) suggests that the criminality of bribery "is surprisingly difficult to explain" when considering the "harm-doing" of the act, because some bribes cause no apparent harm. Horder contends that the criminal justification for bribery relies on the "nature and degree of remote harm" potentially resulting from a bribe resulting in no sanction. If there is no punishment, then there would be no deterrence, but as deterrence is difficult to measure, this results in a "potentially problematic case" for determining such a criminal act. Private security agents are no less susceptible to such deterrence, but if punishment is not certain, then the deterrent effect would be difficult to measure (Paternoster 2010).

Green (2005) characterizes bribery as a "bilateral agreement between 2 parties" wherein "the briber gives or offers something of value in exchange for the bribee's agreeing to act on the briber's behalf." The person bribed transgresses against a duty to his or her position, and the briber "commits the morally wrongful act" by corrupting the bribee. Security personnel are often disadvantaged in such a way, and as they are licensed by the government in most states, they are liable to be prosecuted for certain forms of bribery (such as transactions that involve criminal acts on a client's property) and possible loss of their licenses.

Conclusion

Bribery is leverage. It is the result of an exchange between two or more parties, such that each needs something from the other. The lever is the thing to be exchanged, desired by the bribee (the person or entity accepting the bribe) and offered by the briber (the person or entity doing the bribing), in return for something of value desired by the briber. This basic process holds true for the bribe at its many levels, including security. Those working in security are in positions of trust, guard people and assets, and are therefore targets for those who seek to profit from the venue protected by private security professionals. The opportunity and risk for bribery are ever present and must be guarded against.

Cross-References

- ▶ Investigations: Criminal
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Exterior Application
- ▶ Physical Security: Interior Applications
- ▶ Protection and Security in Public Spaces
- ▶ Residential Security: Gated Communities
- ▶ Residential Security: Houses and Apartments, Public and Private
- ▶ Retail Security: Use of Security Guards
- ▶ Security Management
- ▶ Security: Proprietary

References

Carson, T. L. (1987). Bribery and implicit agreements: A reply to Philips. *Journal of Business Ethics, 6*(2), 123–125.

Cornell Law School. (n.d.). *Terry v. Ohio*. https://www.law.cornell.edu/supremecourt/text/392/1

D'Andrade, K. (1985). Bribery. *Journal of Business Ethics, 4*(4), 239–248.

Green, S. P. (2005). What's wrong with bribery? In R. A. Duff & S. P. Green (Eds.), *Defining crimes: Essays on the criminal Law's special part*. Oxford: Oxford University Press.

Horder, J. (2011). Bribery as a form of criminal wrongdoing. *Law Quarterly Review, 127*, 37–54. London: Sweet & Maxwell.

Noonan, J. T., Jr. (1984). *Bribes: The intellectual history of a moral idea*. New York: Macmillan.

Paternoster, R. (2010). How much do we really know about criminal deterrence? *The Journal of Criminal Law and Criminology, 100*, 765–824.

Stein, A. (2012). *Corrupt intentions: Bribery, unlawful gratuity, and honest-services fraud*. Accessed at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://search.yahoo.com/&httpsredir=1&article=1668&context=lcp

Wollan, M. (2016). *How to make a citizen's arrest*. New York Times Magazine. https://www.nytimes.com/2016/05/08/magazine/how-to-make-a-citizens-arrest.html

Further Reading

Lambsdorff, J. G. (2007). *The institutional economics of corruption and reform: Theory evidence and policy.* Cambridge: Cambridge University Press.

Langsted, L. B. (2009). Bribery, bribery across borders and the like from a Danish perspective. *Scandinavian Studies in Law, 54*(13), 247–268.

Bus Security

Dorothy Moses Schulz
Law, Police Science, and Criminal Justice Administration, John Jay College of Criminal Justice (CUNY), New York, NY, USA

Keywords

Crime Prevention Through Environmental Design (CPTED) · Closed circuit video surveillance (CCTV) · Operator assaults

Definition

Bus (motor coach) security is comprised of the procedures and activities to protect equipment, facilities, employees, and patrons of bus companies from harm; it includes efforts to prevent, mitigate, respond to, and recover from incidents that may occur on vehicles, at terminals and waiting areas, or others areas for which bus companies are responsible.

Introduction

Assessing security needs and responses of bus systems is challenged by the large number and types of bus systems operating in North America. Security for buses has received less attention than for other transit modes (such as air or rail travel). With few exceptions, bus security is less focused on violent and terrorist-related crimes than on public order offenses in stations, waiting rooms, and on vehicles, and with crimes against the transit system itself such as vandalism, theft of fares, assaults on bus operators, and sometimes vehicle hijackings (Bus Safety Data Report 2018). Also, because bus systems are unlikely to have their own police departments, serious crimes are reported to the local police and nonserious security events (i.e., fare evasion or patron fights that do not result in injury) often go unreported (Schulz and Gilbert 2011).

Most people define a "bus" simply as a vehicle that runs on streets and picks up and discharges passengers; however, within the transit industry, bus systems vary by type of service (local, commuter, long-distance, or school) and whether they are public or private (Fact Book 2017). Local bus service involves travel within a city or county on fixed-routes (the same route and stops on all trips); demand-response (vans arrive when called to take a patron to a specific destination), and commuter buses, which primarily connect suburban areas with the central business district. These are overseen in the United States by the Federal Transit Administration (FTA), part of the Department of Transportation (USDOT), and in Canada by Transport Canada (TC). There are also hundreds of long-distance (also called intercity) bus systems; among the best known are Greyhound, Trailways Lines, and Peter Pan, which serve about 4,000 communities in the United States (Walsh 2003). Leisure and charter buses are considered intercity carriers. In the United States, the Federal Motor Carrier Safety Administration (FMCSA), part of USDOT, and in Canada, TC, together with the provincial governments, regulate these buses. School buses, which may be used only to transport students to/from school or for school-related activities, are regulated in the United States by the National Highway Traffic Safety Administration (NHTSA), also part of USDOT, and in Canada by TC.

The American Public Transportation Association (APTA) estimates that not including school and intercity buses, buses operate over 230,000 miles of streets and roads in the United States and in 2014 employed about 300,000 people (Fact Book 2017). TC estimates that 15,000 buses are operated in Canada by about 1,500 different providers employing about 9,000 people, primarily as drivers (Road Transport n.d.; CUPE Fact Sheet 2017). No central repository of

crime data exists in either country. In the United States, the FTA maintains a National Transit Database (NTD), but greater emphasis is placed on safety than on security and reporting is not mandatory. Despite the industry fragmentation, government reports, agency documents, and media coverage have highlighted common security problems and solutions among bus systems. This entry describes security issues facing North American bus systems and discusses crime prevention interventions and strategies employed by most of them to counter criminal activity.

Crime Prevention Through Environmental Design (CPTED), Closed Circuit Video Surveillance (CCTV), and Communications Enhancements

Beginning in the 1970s and intensifying in the 1980s and 1990s, transit systems recognized crime and public order problems, including loitering by nonpatrons, homeless persons, and unruly teenagers; fare payment evaders who harassed bus operators and other patrons; and graffiti on the equipment, in stations, and on bus shelters. To counter disorder, agencies adopted crime prevention though environmental design (CPTED) principles, such as improving lighting in yards and public facilities, adding fencing to bus garages, and installing electronic closed circuit video surveillance (CCTV) to monitor their property (Schulz and Gilbert 2011).

In stations, bus systems rearranged furnishing to minimize hiding places, and to curtail loitering they installed slanted seat or separated benches to prevent stretching out across three or four seats. Keeping bus transfer points and buses clean became a priority as did preventing graffiti or scratchiti (etching rather than spray painting onto surfaces). Small systems, with small security budgets, discovered that playing classical or other soothing music deterred rowdy teenagers, whose noise and boisterousness often frightened other patrons, particularly the elderly, from frequenting the stations. System operators often have little control over on-street bus shelters, since most are not responsible for their care or cleanliness, but many have worked with local jurisdictions to enhance housekeeping in and around shelters and to minimize advertising and other signage that blocks benches from view (Schulz and Gilbert 2011).

Other countermeasures include public awareness campaigns; increased patrols by law enforcement or security personnel; legislative efforts to increase penalties for assaults on drivers; and technological solutions, particularly CCTV and devices that allow operators to report suspicious or dangerous behavior without alerting the perpetrator or other passengers (Tools and Strategies 2018). Bus systems rely heavily on CCTV onboard vehicles, in large stations and transportation centers, in parking facilities, and in bus garages. Between 2001 and 2015, the percentage of buses equipped with CCTV increased from 13% to 73% (Fact Book 2017). Interior cameras (in the buses facing patrons) are generally publicized by signage to enhance patron security by deterring criminal behavior although the video is also used to support or refute accident or injury insurance claims (Tools and Strategies 2018). External cameras (facing outside the bus) may record patrons sneaking onboard without paying but are used primarily to investigate accidents.

Other security enhancements are intended to increase communication between a bus operator and a central command center and between a bus operator and patrons. For instance, providing operators with two-way radios allows them to report when they need supervisory or police intervention. Automatic vehicle location (AVL) equipment, similar to a global position system (GPS) but tied to a particular vehicle, allows agencies to know immediately if buses have left their assigned route. Tracking a bus that has reported a security problem makes it easier for police to develop response strategies (Schulz and Gilbert 2011; Tools and Strategies 2018). In addition to security, AVL can also provide information to passengers waiting for vehicles.

Public address systems, automated stop announcements, and passenger-operator intercoms also serve a dual purpose of keeping passengers informed and increasing the security of the trip (Schulz and Gilbert 2011; Tools and Strategies 2018). Many systems have programed

their exterior destination signs to flash "Call 911" upon operator activation. If the operator cannot safely communicate with a command center, it is anticipated that someone on the street or roadway will inform the police that the bus is in trouble.

Industry associations are active in developing security strategies. Together with the American Association of State Highway and Transportation Officials (AASHTO), APTA, and the Community Transportation Association of America (CTAA), the FTA administers a voluntary safety and security program that offers audits by expert practitioners and checklists that can be used to evaluate safety, security, and emergency preparedness programs; publishes best practices, and sponsors conferences and seminars. In Canada, TC collaborates with bus operators, the Canadian Urban Transit Association (CUTA), and Motor Coach Canada (MCC) to develop information on risk assessments; employee training; exercises and drills; writing and maintaining security plans, and creating public awareness campaigns (Road Transport n.d.).

Fare Policies, Fare Evasion, and Operator Assaults

Most violent crime on buses in the United States and Canada stems from fare evasion or transfer policies, which result not only in lost revenue but in assaults on bus operators who challenge patrons refusing to pay their fares (Bus Drivers under Attack n.d.). To minimize these thefts and arguments, many systems accept only exact or prepaid fares, with no cash accepted on the vehicle. Systems have found that a single fare for an entire trip, rather than zoned fares that depend on distance, minimize driver/patron disputes (Stern 1997; Larwin and Koprowski 2012). Many buses operate with proof-of-payment systems that allow patrons to board without showing a ticket but who may be asked to show it to fare enforcement officers who board the vehicles periodically to make such checks. Enforcement officers are generally authorized to ask patrons to exit the bus if they have no ticket or, if the enforcement agents' handheld computer indicates a repeat offender, to issue a citation for fare evasion (Schulz and Gilbert 2011; Larwin and Koprowski 2012).

Attacks on operators have been the impetus for the installation of cameras on buses and of driver safety partitions. For example, New York City began installing cameras in 2011 in response to a 20% spike in operator assaults compared to the previous year. Earlier, in 2008, a driver was killed after refusing a nonpaying patron a free transfer, leading operators to more actively report victimizations (Permino 2012). Similarly, the Los Angeles Metro bus system added surveillance equipment and plastic barriers separating drivers from patrons in 2015 after a 35% increase in driver assaults between 2012 and 2015, including 138 assaults in 2014, a third of which began as fare disputes (Metro to Raise Security. . . 2015).

Transit systems and unions representing drivers have been successful in lobbying states to increase criminal penalties for assaults on operators. According to the Amalgamated Transit Union (ATU), which represents about 200,000 members in 45 states and nine Canadian provinces, 30 states have enacted such legislation (Bus Drivers under Attack n.d.). Riders in many cities are familiar with signs reminding them that assaulting a bus driver is a felony.

Bus crimes not involving operators are similar to crimes occurring in other public space. They range from violence involving passengers to violence that starts on the street but carries over into the bus. An example of the latter was a dispute near a Honolulu, Hawaii, bus stop in March 2015 that led a group of individuals to ask a driver to help them escape from a reportedly armed group chasing them. The driver permitted them to enter the bus, but when he denied entry to the second group, they attacked the bus, shattering windows and the windshield (Driver Hailed as Hero. . .2015). While these incidents receive local media attention and are highlighted by unions representing operators and by rider advocate groups, estimating how often they occur is virtually impossible.

Hijackings

Bus hijackings of local public buses, long-distance private buses, and school buses are rare.

Because of each one's unique circumstances, they are difficult to classify or prevent. Many result from riders' behavioral or psychological problems. For example, an intercity bus hijacking at John F. Kennedy airport in 1977 which resulted in two passengers being killed and two wounded, involved a gunman who told police he was "fed up with society" before being taken into custody after a 13-hour standoff (Bus hijacker kills 2… 2017). In 2012, a drunken patron who hijacked a Greyhound bus traveling from Washington, DC, to Miami, was sentenced to more than 19 years in prison after pulling a pellet gun on the driver and demanding to get off the bus. Here, after the hijacker threatened other passengers, the driver complied with instructions to allow them to exit the bus. When the hijacker allowed the driver to also exit to use a gas station restroom, law enforcement personnel surrounded the bus and subdued him (Rockwell 2012).

A number of hijackings of occupied school buses have received vast media attention due to what effectively becomes the kidnapping of young children. An early case that received much notoriety occurred in July 1976, when 26 children between the ages of 5 and 14 and their bus driver were kidnapped in Chowchilla, CA, by armed men blocking the bus's route. The students, who were attending an elementary school summer session, were being dropped off on their way back from a field trip. The kidnappers hid the bus and drove the children and their driver around in two vans for almost 12-hour before taking them to a quarry, from which the driver and the children ultimately escaped. Although the three kidnappers, who were all caught, tried, and sentenced to life in prison, had attempted to make ransom calls, they were unable to do so because the local telephone lines to the police were tied up by media calls and families searching for their children. The arrests were a result of the bus driver, under hypnosis, remembering the license plate number of one of the vans (Lindsey 1976; Baugh 1979). The incident was the basis of a number of television programs, including in 1993 an ABC Network 2-hour special, *They've Taken Our Children* (2019) and in 2015 on the cable network Investigation Discovery (*House of Horrors: Kidnapped*). The case received renewed media attention in 2016, when a lawsuit was filed on behalf of the victims after two of the three kidnappers were paroled, one in 2013 and another in 2015 (Chowchilla school bus… 2016). Another case involved an armed school bus driver who took 13 children from rural Pennsylvania on an unauthorized 6-hour, 115-mile "field trip." None of the children was physically harmed, and although many indicated they were frightened, at least one was quoted as saying "we were having fun." During arraignment, it was determined that the driver had been treated for psychiatric problems and had recently stopped taking his medication (Court Orders Psychiatric…2002; Bus Driver Faces…2015).

The randomness of these events contributes to the difficulty preventing them. For instance, in 2013, a knife-wielding man hijacked 11 elementary-school-age children and their bus driver. With no apparent motive, after a woman had denied his demand outside an apartment complex to be given a vehicle, he jumped onto the bus. Although armed with a knife, he made no threats against the driver or the children. After a chase by local police, he was removed from the vehicle and charged with vehicle piracy, kidnapping, and aggravated assault (Huynh and Lesnick 2013). In another case, in 2018, near Fresno, CA, a man hopped onto a bus carrying more than 40 elementary school children when the driver stopped so students could use a restroom. While a teacher escorted two students to the restroom, the assailant jumped onto the bus and tried to yank the driver from her seat but she removed the keys from the ignition and hid them. Although the hijacker had previously been charged with attempted carjacking and attempted kidnapping, based on his statements, police authorities believed that might have had mental health issues (Darrah 2018).

Hijackings sometimes involve former or want-to-be employees; in New York City, in 2016, a former bus driver took a vehicle for a "joyride" after being asked not to smoke on a bus. Also in the New York area, Darius McCollum, who suffers from Asperger syndrome, has posed as a subway motorman or bus driver to take over

New York subway and buses, New Jersey Transit buses, and Greyhound buses at least 30 times, resulting in his being incarcerated 19 times. Despite no one being harmed by McCollum, the ease with which he has entered garages or unattended equipment raises questions about the success of existing security measures (*Off the Rails* 2016).

Terrorist Activity

Discussions of terrorist activity at mass transit generally do not separate buses from rail and do not clearly distinguish between domestic and international events. Terrorist actions against buses occur frequently in Israel, India, Pakistan, and the Russian Federation. The Mineta Transportation Institute (MTI) Database on Terrorist and Serious Criminal Attacks Against Public Surface Transportation counted over 3,000 attacks against public transportation between January 1, 1970 and January 23, 2012. Of these, 47.4% were against buses, bus stations, and bus stops (Butterworth et al. 2012, p. 3), but none were in the United States or Canada. A more recent account of terrorist activity targeting US transportation systems between 1970 and 2015 counted 89 attacks; none involving buses (Miller 2016). Two recent incidents also illustrate problems in defining a terrorist-related event and the actual target.

In New York City, in December 2017, an explosion occurred in a passageway connecting the Times Square subway station with the Port of New York and New Jersey's (PANYNJ) Bus Terminal at Eighth Avenue and 42nd Street during the morning rush hour. The suspect, who, according to police, acted on behalf of the Islamic State, was convicted 11 months later; it was never clear whether he was targeting the subways, the bus system, either, or both (Weiser and Palmer 2018). In January 2018, a Mexican national in the U.S. illegally, who was on a Greyhound bus traveling through the Midwest threatened to kill law enforcement personnel. Although he was charged with making terrorist threats because he mentioned law enforcement, it is unclear whether this was actually a terrorism-related incident (Fox6news 2018).

Despite the dearth of terrorist-related threats to buses, an Intercity Bus Security Grant Program (IBSGP) established by the 9/11 Commission Act of 2007 and administered by the Federal Emergency Management Agency (FEMA) provides funds for anti-terrorism activities. The 2015 and 2016 funding was $ 3 million; for 2017 and 2018, it was reduced to $ 2 million. After meeting the Department of Homeland Security (DHS) requirements, systems may apply for funds to upgrade physical security at bus stations and maintenance facilities and for airport-like passenger and baggage screening. Critics of IBSGP note that it has never been fully funded and that funds are disbursed only to agencies that have demonstrated to FEMA that they have credible security plans and will use the funds to advance a specific security program (Burtwistle 2017).

The Transportation Security Administration (TSA) funds bus anti-terrorist training programs for employees, especially drivers, and periodically works with bus systems to set up security checkpoints in stations. With the exception of some intercity buses, screening of bus and rail patrons on a regular basis has not been successful. These travelers expect quick entry and exit from the coaches and to carry their luggage onto the vehicle or place it nearby. Even if such measures were in place, they would not prevent external attacks such as bombs placed in the road, carried in vehicles traveling adjacent to the bus routes or rail lines, or hijackings.

Drug Interdiction and Immigration Enforcement on Buses

Controversy surrounds police officers' authority under the Fourth Amendment to search and seize contraband on public buses. Early activity and Supreme Court cases in this area were centered on drug interdiction but the authority has been used more recently for immigration checks on passengers. Inconsistent drug-related decisions led ultimately to the *U.S. v. Drayton* (122 US

2105, 2002), which involved two drug seizures from two individuals on the same bus. The Court ruled that officers are not required by the Fourth Amendment to "advise bus passengers of their right not to cooperate and to refuse consent to search" (*Drayton* 2002, p. 2107). The decision has been the basis for Customs and Border Patrol (CBP) agents to board buses to check patrons' immigration status. The checks, primarily on intercity buses and sometimes on local public buses, generally result in those being taken into custody being turned over to Immigration and Customs Enforcement (ICE) for detention and possible deportation. Although a coalition of groups led by the American Civil Liberties Union (ACLU) has demanded that Greyhound stop immigration enforcement, the company says it has no choice, that it does not cooperate with CBP agents, and that the searches have negatively impacted both its customers and its operations (Hayoun 2018).

Conclusion

Measuring the number and type of security incidents on buses is impossible due to decentralized reporting systems and the different responses by operators and local jurisdictions. Although FTA's NTD captures some data, its definition of a "security event" as one "where a person causes harm to themselves, or another person or damage to property, including suicides, assaults, and bomb threats" (Bus Safety Data Report 2018) differs from law enforcement definitions. In addition, because many bus systems do not report to NTD, it is difficult to interpret the data as reflective of trends in security incidents occurring on buses. Despite these difficulties, bus systems have been and continue enhancing security for equipment, operators, and patrons primarily through CPTED, CCTV, and other technological means.

Cross-References

- ▶ Critical Infrastructure: Transportation Systems
- ▶ Rail (Train) Security

References

Baugh, J. W. (1979). *Why have they taken our children? Chowchilla, July 15, 1976*. New York: Dell Publishing.

Burtwistle, L. (2017, June 21). Congress should fully fund the intercity bus security grant program. The Hill. https://thehill.com/blogs/congress-blog/politics/33870. Accessed 24 Sept 2018.

Bus Driver Faces Kidnapping Charges, Psychiatric Evaluation. (2015, January 13, updated). Fox News. https://www.foxnews.com/story/bus-driver-faces-kidnapping-charges-psychiatric-evaluation. Accessed 19 March 2019.

Bus Drivers under Attack. (n.d.). Silver Spring: Amalgamated Transit Union (ATU).

Bus Hijacker Kills 2 at JFK before Being Arrested in 1977. (2017, July 5). *New York Daily News*.

Bus Safety Data Report 2008–2016 (2018, November). Washington, DC: Department of Transportation.

Butterworth, B. R., Dolev, S., & Jenkins, B. M. (2012). *Security awareness for public bus transportation: Case studies of attacks against the Israeli Public Bus System*. San Jose: Mineta Transportation Institute.

Chowchilla School Bus Kidnap Victims File Lawsuit 40 Years After Abduction. (2016, March 25). https://abc30.com/new/chowchilla-school-bus-kidnap-victims-file-lawsuit-1262680. Accessed 19 Mar 2019.

Court Orders Psychiatric Evaluation for Bus Driver Charged in Kidnapping. (2002, January 26). *The New York Times.*

CUPE Fact Sheet. (2017, July 12) Canadian Union of Public Employees (CUPE). https://supe.ca/fact-sheet-public-transit-privitazation-and-canda-infrastructure-bank. Accessed 30 Dec 2018.

Darrah, N. (2018, November 7). California Man Charged with Attempted Kidnapping after Hopping on Bus Full of Schoolchildren. FoxNews. https://www.foxnews.com/us/california-man-charged-with-attempted-kidnapping-after-hopping-on-bus-full-of-schoolchildren. Accessed 22 Mar 2019.

Driver hailed as hero after city bus attack. (2015, March 23). http://www.kitv.com/news/driver-hailed-as-hero-after-city-bus-attack/31977428. Accessed 30 Dec 2018.

Fact Book. (2017, February). Washington, DC: American Public Transportation Association.

Fox6news. (2018, January 13). https://fox6news.com/2018/01/13/man-on-greyhound-bus-threatened-to-kill-was-in-US-illeg.... Accessed 31 Jan 2019.

Hayoun, M. (2018, October 24). Immigrant Rights Groups Are at Odds with Greyhound over its Right to Forbid Immigrant Enforcement from Entering Buses, Pacific Standard. https://psmag.com/social-justice/immigrant-rights-groups-are-at-odds-with-greyound-ov. . . . Accessed 27 Oct 2018.

House of Horrors: Kidnapped. (Buried Alive TV episode) https://www.imdb.com/title/tt4527418). Accessed 25 Mar 2019.

Huynh, C. & G. Lesnick. (2013, October 17). School bus carjacked in jacksonville; Children safe. https://www.arkansasonline.com/news/2013/oct/17/school-bus-carjacked-jacksonville-chil. . .. Accessed 19 Mar 2019.

Larwin, T. F., & Koprowski, Y. (2012). *Off-board fare payment using proof-of-payment verification*. Washington, DC: Transit Cooperative Research Program (TCRP) Synthesis 96.
Lindsey, R. (1976, July 17). 26 Children found safe after Being kidnapped from bus in California. *The New York Times*.
Metro to Raise Security on Buses. (2015, March 26). http://egpnews.com/2015/03/metro-to-raise-security-on-buses. Accessed 30 Dec 2018.
Miller, E. (2016). Terrorist attacks targeting critical infrastructure in the United States, 1970–2015. College Park: START.
Off the Rails: The Darius McCollum Story. (2016, April 7). Adam Irving, Director.
Permino, J. (2012, December 6). Picture this – Safer buses, MTA's Camera Campaign. *The New York Post*.
Road Transport, Government of Canada. (n.d.). https://www.tc.gc.ca/eng/policy/anre-menu-2021.htm. Accessed 7 Jan 2019.
Rockwell, M. (2012, June 29). El Salvadoran man gets more than 19 Years in Prison for Bus Hijack in North Carolina. *Government Security News*. http://www.gsnmagazine.com/article/26665. Accessed 2 July 2012.
Schulz, D. M., & Gilbert, S. (2011). *Video surveillance uses by rail transit agencies*. Washington, DC: Transit Cooperative Research Program (TCRP) Synthesis 90.
Stern, R. (1997). *Bus transit fare collection practices*. Washington, DC: National Academy Press.
*They've Taken Our Child*ren. https://www.imdb.com/title/tt0105576. Accessed 25 Mar 2019.
Tools and Strategies for Eliminating Assaults Against Transit Operators. Volume 1: Research Overview. (2018). Washington, DC: Transit Cooperative Research Program (TCRP) Synthesis 193.
U.S. v. Drayton, 122 U.S. 2105 (2002).
Walsh, M. (2003). The Bus Industry in the United States. R. Whaples, Ed., EH.Net Encyclopedia. http://eh.net.encyclopedia/the-bus-indistry-in-the-unted-states. Accessed 7 Jan 2019.
Weiser, B. & Palmer, E.. (2018, November 6). Akayed Ullah Guilty of ISIS-Inspired Bombing. *The New York Times*.

Further Reading

Bus and Coach Security Recommended Best Practice. (2018, July, 3rd ed). London: Department of Transport.
FTA Bus Safety Program. https://www.transit.dot.gov/regulations-andguidance/safety/bus-safety-program. Accessed 15 Dec 2018.
Hambridge, N. B, Howitt, A.M., & Giles, D.W.. (2017, April). Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies. *Homeland Security Affairs* 13, Article 2.
Thompson, B., Matos, I., & Previdi, J. (2016). *On board camera applications for buses*. Washington, DC: Transit Cooperative Research Program (TCRP) Synthesis 123.

Business Continuity Plan

Malcolm B. Reid
College of Graduate and Continuing Studies, Norwich University, Northfield, VT, USA

Keywords
Business continuity management (BCM) · Business continuity plan (BCP) · Business impact analysis

Definition

ISO 22301 defines the business continuity plan as "documented procedures that guide organizations to respond, recover, resume, and restore to a predefined level of operation following disruption."

Introduction

Business continuity is the practice of preplanning for disruptive events that could negatively impact an organization and its stakeholders. It provides a framework for timely recovery of operations following a disruption that minimizes the negative impacts. Business continuity planning (BCP) is similar to Continuity of Operations Planning (COOP). COOP is used in the public sector for continuity of government whereas BCP is generally used by the private sector. According to NFPA (2019) "the most significant difference between BCP and COOP lies with objectives and the definition of critical or essential functions and how demand for public sector essential services could change during an incident". The business continuity plan provides a playbook designed to guide action in the event of a disruption.

All organizations should develop, maintain, and exercise their business continuity plan. The process of business continuity planning begins with analysis which includes the business impact analysis and risk assessment. The BIA identifies and prioritizes critical functions, while the risk assessment identifies and prioritizes likely threats

Business Continuity Plan, Fig. 1 Process for BCP development and improvement

to those critical functions. Business continuity strategies and BCPs are documented based on the analysis outputs. Documented plans must be validated and rehearsed through exercising to be reliable. Lessons learned from actual events and exercises can be used to update plans for continual improvement (Fig. 1).

Business Impact Analysis

The business impact analysis (BIA) provides essential information for developing the business continuity plan. The BIA assesses impacts of a disruption on an organization including consideration of potential damage to reputation, market share, operational effectiveness, or stakeholder relationships along with resource requirements to continue or recover from a disruption (NFPA 2019). Resource requirements that should be considered include "Personnel, Equipment, Infrastructure, Technology, Information, and Supply Chain" (NFPA 2019).

The BIA also determines timelines for recovery including the Maximum Tolerable Period of Disruption (MTPD), the Recovery Time Objective (RTO), and the Recovery Point Objective (RPO). The MTPD is defined by ISO 22301 as the "time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable." MTPD is also referred to as the Maximum Tolerable Outage or Maximum Acceptable Outage. The RTO is the targeted time for recovery of the product, service, activity, or resource which should be less than the MTPD to avoid unacceptable impacts (ISO 22301). The RPO identifies the maximum data loss and the point to information should be restored to in order for activities to operate following a disaster (ISO 22301).

In addition to evaluating the impacts of a disruption over time, the BIA identifies essential supporting business processes and dependencies for each critical function. Interdependencies of processes are also considered. The primary categories of dependencies are:

- Workforce – Skills and minimum number personnel to execute BCP procedures.
- Facilities – Buildings including office space, data centers, or manufacturing space.
- IT infrastructure – Servers and their configuration requirements, networking dependencies, this may include Cloud-based solutions.
- Data – Information backup requirements to support the critical functions (paper, data, backup arrangements, security and storage requirements).
- Third party providers – Any critical dependencies provided by third parties must be identified.

Based on information gathered in the BIA, business continuity plans are designed to achieve the RTO and RPO with consideration for the resource requirements and organizational constraints. This approach enables an organization to effectively balance the cost and effectiveness of continuity strategies while mitigating unacceptable impacts.

The risk assessment complements the BIA by identifying threats and risks associated with the prioritized activities and resource requirements. The risk assessment also identifies Single Points of Failure (SPOFs) through following process flow and dependencies to map (Bryant 2013).

Based on findings from the risk assessment, the continuity strategy identifies measures that will reduce likelihood and impact of prioritized likely threats to critical functions.

Business Continuity Strategy

The plan should include a continuity strategy that meets the requirements identified in the business impact analysis. The strategy is the overall approach to continuity and recovery. Strategies address loss of critical resources identified in the BIA. Strategy is selected based on its ability to achieve the RTO and RPO and in alignment with the organization's resource capability. Strategies that deliver the greatest resilience and speediest recovery are often the most expensive unless they are aligned with business as usual ways of working. Table 1 outlines common strategies.

There are additional strategies and variations of these strategies which can be adapted to the organization's specific requirements.

Roles and Responsibilities

The incident response structure provides a management structure and procedures for response to disruptions. According to the BCI (2018), the response structure provides "established command, control and communication systems to ensure that the organization has a clearly documented and well understood mechanism for responding to an incident, regardless of its cause." The response structure activates the business continuity response in accordance with established processes and procedures for "activation, operation, coordination, and communication of the response" (ISO22301). The response structure should align with the organization's normal organizational structure.

Responsibilities include communication, coordination, and specific actions that must be carried out to facilitate the recovery. The Incident Command System (ICS) model has been widely adopted for development of an incident response structure. The ICS was developed to provide a common organizational structure covering all functions required for effective emergency response (Bigley and Roberts 2001).

Internal and external communications are particularly critical roles in the business continuity response. Internal communication involves keeping the workforce up-to-date on the disruption and business continuity response and their expected actions. External communication is directed at stakeholders and the media.

Business Continuity Plan, Table 1 Business continuity plan recovery strategies

Strategy	Addresses loss of	Examples	Relevant disruption scenarios
Remote working/ telework	Location	Employees work from home or other locations by connecting to the Internet to access corporate resources usually via VPN	Physical disruptions at primary facilities where application dependencies are not impacted Not effective against cyber attacks or people disruptions such as pandemics
Process transfer	Location and people	Organizations that carryout processes at multiple locations can shift work to another location if the capacity is available or can be increased for the duration of the disruption	Physical disruptions where local internet connectivity is not available or local people disruptions
Alternate location	Location	Employees relocate to another location not impacted by the disruption. Organizations with multiple locations may be able to leverage their additional facilities. Organizations may also engage third-party providers who specialize in providing hot or warm standby sites equipped with relevant working requirements	Physical disruptions including natural disasters

Plan Documentation

The first priority in a business continuity plan is the health and safety of personnel.

The plan provides documented procedures for response to a disruption and how the organization will continue or recover within the agreed RTO. The plan is a playbook for the individuals and teams with identified roles and responsibilities in the continuity and recovery. Once the plan has been documented, it must be communicated to relevant parties particularly all individuals with roles and responsibilities defined within the plan. Plans should be available for reference in an actual disruption either in hard copy or electronically.

The BCI (2018) recommends that plans should be direct, adaptable, concise, and relevant to make them focused and user-friendly in high pressure disruptions.

Phases of business continuity guided by the plan include:

1. Activation
2. Execution

Plans may also cover the reconstitution phase to guide return to normal operations. This includes procedures to return to business as usual after the disruption has concluded.

The plans should document assumptions, roles and responsibilities, escalation and delegation processes, and liaisons for external organizations (NFPA). According to ISO 22301 (ISO 2012) and ASIS BCM, "Each plan shall define purpose and scope, objectives, activation criteria and procedures, implementation procedures, roles, responsibilities, and authorities, communication requirements and procedures, internal and external interdependencies and interactions, resource requirements, and information flow and documentation processes."

Recovery Procedures

(a) Sequence of activities for overall coordination and management of the disruption based on priorities
(b) Specific actions that must be taken to meet the recovery time objective
(c) Escalation/awareness

Contact details for all personnel with roles and responsibilities in the plan should be included and kept up-to-date regularly.

Additional information that may be included in your plan includes:

- Site maps for facilities
- IT architecture diagrams
- Special instructions for recovery tools

Research findings of a study conducted on BCP implementation identified the most effective aspects of the plans as "identification of critical functions, communications plan, information back-ups, and training and testing" (Hatton et al. 2016).

The plan is sometimes called a playbook because it provides the team with guidance on actions to take in a disruption. The level of detail required for the plan depends on the complexity of procedures that must be carried out.

Plan Activation/Exercising

Once the plan is documented, recovery teams must be prepared for plan activation. Exercising is the best way to prepare teams for an actual disruption and invocation of the plans. The business continuity procedures require exercising to provide all team members with recovery roles and responsibilities, an opportunity to practice their response, validate plans, and identify improvements. In addition to validation of plans, exercises can also provide capacity testing and awareness for internal and external stakeholders (ASIS BCM).

Procedures for plan activation should be included in the business continuity plan under the section on "activation criteria and procedures." Activation procedures should clearly state the authorized decision makers and conditions and are required to invoke the business continuity plan. The procedures should define disruption thresholds that guide activation of the plan. The impact thresholds which guide decision makers in invocation of the plan should align with the organization's priorities and business

continuity requirements such as number of customers impacted or length of the disruption in hours or days impacting prioritized activities and critical dependencies (BCI 2018). The activation procedures should include a process for assessing the actual impact of the disruption on "people, property, operations, or the environment" (NFPA 2019). Documenting clear guidelines for activation supports sense making in potentially stressful situations where decision making can be degraded. Well before the disruption occurs, "staff must be given frameworks that they can use to correctly interpret what they see and experience when things go wrong" (Oberlin 2017).

An emergency operations center (EOC) is established on activation of the business continuity plan to maintain communications and coordination with incident command (NFPA 2019). The EOC may be established in a physical meeting room or using virtual meeting solutions. The EOC remains in operation for the duration of the disruption. In a disruption, collaboration is required for an effective response. The EOC is primarily responsible for maintaining coordination. Collaborative exercises with the EOC activated are recommended to improve communication and coordination between teams.

Exercises and tests provide an opportunity for individuals and teams to practice their business continuity roles and responsibilities including coordination while also assessing plan effectiveness. There are several different approaches to exercising beginning with discussion-based exercises and culminating in full scale rehearsal exercises. Exercise objectives are defined for each exercise during exercise planning to clarify aims and expectations.

Expected outcomes linked to core capabilities are identified in the exercise objectives. The exercise structure and scenario should facilitate achievement of the objectives. Evaluation of the exercise is based on performance of the participants in respect to the exercise objectives. Directly following the exercise, a debriefing is conducted to capture participant impressions and recommendations.

An exercise report is compiled to document the exercise evaluation and capture lessons learned shared in the debrief and evaluation. Similarly, after an actual event a review of the recovery is conducted to identify gaps in capabilities, or plan procedures and make recommendations for improvement. A program of continuous improvement is required to deliver plans that can work in an actual disruption. Lessons learned are captured following an actual incident or exercise. Action plans for improvement are developed based on lessons learned.

Conclusion

Business continuity facilitates recovery from a variety of threats both intentional and unintentional. An all-hazards approach is recommended which focuses on response to disruptions of critical resources and therefore can be adapted to any scenario including natural disasters, structural failures, human errors, and cyber-attacks. BCP priorities should be aligned with the organization's strategic priorities including customer/stakeholder requirements, legal and regulatory requirements, and organizational policy.

Cross-References

- ▶ Emergency Management: Crisis Communication
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Incident Command System
- ▶ Emergency Management: Preparedness and Planning

References

ASIS/BSI BCM.01-2010, Business continuity management systems – Requirements with guidance for use.

BCI. (2018). *Good practice guidelines*. The Business Continuity Institute (UK), Berkshire, UK.

Bigley, G., & Roberts, K. (2001). The incident command system: High-reliability organizing for complex and volatile task environments. *The Academy of Management Journal, 44*(6), 1281–1299. Academy of Management. Retrieved 17 Mar 2019, from http://ccrm.

berkeley.edu/pdfs_papers/Bigley_Roberts_CommandSystem.pdf
Bryant, R. (2013). Identifying single points of failure in your organization. *Journal of Business Continuity & Emergency Planning, 7*(1), 26–32.
Hatton, T., Grimshaw, E., Vargo, J., & Seville, E. (2016). Lessons from disaster: Creating a business continuity plan that really works. *Journal of Business Continuity & Emergency Planning, 10*(1), 84–92.
International Organization for Standardization. (2012). ISO/IEC 22301:2012: Societal security – Business continuity management systems – Requirements.
NFPA. (2019). *NFPA 1600: Standard on continuity, emergency, and crisis management*. National Fire Protection Association (USA), Quincy, MA.
Oberlin, R. (2017). Improving disaster outcomes with better decision making. *Journal of Business Continuity & Emergency Planning, 11*(2), 279–286.

Further Reading

ISO 22301 https://www.iso.org/standard/75106.htm
NFPA 1600 https://www.nfpa.org/assets/files/aboutthecodes/1600/1600-13-pdf.pdf
The Good Practice Guidelines https://www.thebci.org/training-qualifications/good-practice-guidelines.html#:~:text=The%20Good%20Practice%20Guidelines%20(GPG,raising%20campaigns%20and%20training%20schedules.

C

Celebrity Protection

Robert Matthiessen
Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Close protection · Motorcade and Route Management

Definition

Celebrity protection is the protection of a human asset against harassment, injury, death, and embarrassment.

Introduction

When analyzing celebrity protection, some would argue that it is the same as executive protection, which are all part of the principles and fundamentals of close protection security. There are many variations in the close protection field when it comes to protecting the human asset. As mentioned, the fundamentals and principles remain the same if you are going to ensure an effective protection strategy. However, one difference between providing executive compared to celebrity protection security is the latter's public exposure, but there are other differences between the two.

When analyzing executive protection in comparison with celebrity protection, it should be noted that executives are more reserved and unwilling to engage in extensive public interaction compared to their celebrity counterparts. Most executives are corporate leaders responsible for making important decisions for the company and their shareholders. Their unnecessary exposure can result in danger by an unsuspecting individual. Since there is no immediate need for unnecessary public exposure, executives are primarily shielded from this level of threat. The executive protection professional would advise against unnecessary or high-risk exposure when it is not necessary, and for the most part, the executive usually complies. On the contrary, celebrities for the most part are dependent on their fan base and are more willing to interact and be seen and photographed in public (Holder and Hawley 1998).

This entry will identify celebrity security as the *close protection professional* (*CPP*). If you look at various videos and news reports, celebrities are the most exposed and accessible people in a close protection environment. The ability to navigate crowds and paparazzi in a public space can be very demanding, if not dangerous, for both the celebrity and the CPP. The ability of the CPP to protect a celebrity from harm and/or embarrassment will depend on the training and experience of the CPP to perceive danger, react quickly, but

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

also to remain rational and professional at all times. When celebrities are seen in public, they are usually surrounded by an entourage of staff and security. The differences between executive protection professionals and CPP for celebrities are many times reflected by the security person's size, demeanor, and even attire. Unfortunately, celebrities believe that bigger means better and having large and muscular individuals hovering around them will ensure their safety. This is the farthest from the truth, because close protection security is based on proven tactics, principles, and practices and not presence and behavior.

A nightmare scenario for a celebrity is exiting a location and being surrounded by both fans and paparazzi in an uncontrolled environment. Security in their attempts to keep the crowd away from the celebrity will engage in aggressive behavior toward fans and paparazzi to keep them away from the celebrity. The aggressive behavior exhibited, which may consist of pushing, shoving, or shielding the celebrity from the crowd, can lead to confrontation between security and the public. Tactics or actions like this put the CPP and the celebrity in a dangerous position. The overall problem with this is it can remove security from their position with the celebrity, thus increasing the vulnerability levels for the celebrity. Aggressive behavior by the CPP when it could have been avoided can very well result in an escalated situation that may lead to an assault or injury for the CPP, celebrity, or other people. Incidents like this should not occur, and it is up to the CPP to avoid situations where a crowd can surround the celebrity, thus limiting maneuverability. Training and experience are the most critical tenets for the CPP. They must anticipate potential threats and dangerous environments before risking exposure in an attempt to keep the celebrity safe (Holder and Hawley 1998).

Celebrities come from many different industries, whether music or movies, and each will have a level of tolerance for navigating in the public domain. Celebrities will also want to participate in the party scene and will be exposed to drugs, physical altercations, dangerous weapons, intoxicated fans, and overly aggressive paparazzi. The CPP will be exposed to many dangerous and even criminal environments, in which some celebrities but not executives engage because of mutual friends or other reasons. The CPP must make a decision whether to continue to provide protection, disengage from the celebrity, or attempt to remove the celebrity from a known dangerous environment. The advent of social media increases the overall risk of the celebrity and the CPP as snapchat and other networking application alert fans and stalkers alike of the celebrity's whereabouts. The CPP must use caution when escorting a celebrity and identify potential dangers before entering a public environment. Past experiences should drive the CPP when planning security for the celebrity. Previous locations visited, which resulted in paparazzi and fan attendance, should use advance security personnel to assess and prepare the arrival for the celebrity to reduce the risk of injury to the celebrity and confrontation for the CPP (Oatman 2006). Oftentimes, celebrities will determine how they enter a location, exit a location, or interact with their fans and paparazzi. The CPP who follows orders and direction from the celebrity without analyzing the threat and risk levels is contributing to the dangers that can confront them. The principles and tactics used by protection professionals have been proven to be effective, and the CPP must adhere to them for the safety of all people with or around the celebrity.

Myths and Roles and Responsibility of the Close Protection Professional (CPP)

There are many myths associated with close protection security, and the main one is that the CPP will take a bullet for the person being protected. This is nonsense, as no federal agent, local law enforcement, or private security professional trained in close protection swears to "take a bullet" when assigned to protect a human asset. The main responsibility of the CPP is to remove the celebrity from the danger zone using a cover and evacuate (C&E) method (Oatman 2006). The CPP must always focus on prevention and the avoidance of trouble, rather than combating it. Equally, the CPP must also remain low key, calm, and

rational in many adverse and stressful situations. An effective professional providing close protection security must be able to *analyze the environment* for potential danger before they enter into it. The CPP must maintain continuous levels of training in order to remain effective as a protector of the celebrity. The ability to navigate a crisis situation in a calm and professional manner is attributed to the professionalism, training, experience, and advancements in close protection security training. Changes to the threat environment because of terrorism, social discord, or mental illness continue to change the landscape for celebrities, and it is up to the CPP to meet these security challenges each and every day. The need of the celebrity to interact with the general public is a constant and will require a dedicated and intelligent individual to ensure the safety and security of the celebrity at all times.

Protection strategies must consider threats from criminal groups, fans, and emotionally disturbed people. Many celebrities, even in the face of known threats and increase risk, continue to interact with their fan base both domestically and abroad. It is also important the CPP evaluate both the religious and cultural diversities within the USA and across the globe, as actions or just the appearance of the celebrity can result in increased levels of threat and risk. Anticipating and responding to this type of threat will be a difficult undertaking and will require comprehensive security and countersurveillance planning. The celebrity may become a victim of stalking, or an attack from a fan or mentally ill individual, so the potential danger against the celebrity must be taken seriously. Basic cookie-cutter security planning for a celebrity is not enough, and it will take analysis and comprehensive assessments of known and potential threats to ensure an effective security plan. However, overwhelming the celebrity with convoluted security procedures can equally fail because of frustration on the part of the celebrity to follow the security protocols. The CPP must provide a safe environment for the celebrity that is not overly intrusive, overwhelming, or hindering, as this can result in confusion and possible conflict between the celebrity and the CPP (Oatman 2006).

The CPP must be prepared to explain the security plan to the celebrity, and having good communication skills, manners, intelligence, and common sense will equally contribute to a successful close protection security strategy. This can help in ensuring the security plan is not only approved, but embraced by the celebrity. The CPP must remember that human emotions will come into play when formulating protective security measures; and it is up to the CPP to develop and maintain a professional relationship, not only with the celebrity, but also with the celebrity's family. There is no room for error in protection security as mistakes, redundancy, or complacency will surely result in injury, if not death, for both the celebrity and the CPP. The CPP will be tasked with many requests for services as some may be directly part of their duties and responsibilities and some may not. The CPP must communicate the specific responsibilities to the celebrity and alert anyone who requests or instructs that a service or task that is dangerous or takes the CPP away from performing their primary duties is respectfully refused.

Setting a professional standard early on will ensure the CPP and the celebrity understand what is expected and what is not tolerated. The CPP can be respectful and professional while maintaining the primary role as a protection professional. Once this rule is violated and the CPP begins conducting non-security-related tasks, the effectiveness of the CPP is reduced to being an aide. This will eventually lead to confusion and frustration for the CPP, and it will reduce the overall security environment for the celebrity. The CPP must have their hands free at all times and remain disciplined as to not violate this important rule. Allowing and accommodating the celebrity's requests for carrying packages or holding personal items will result in the CPP becoming disengaged and not focused. It is only a matter of time before a serious incident will occur resulting in injury to the celebrity and the CPP. Though many would differ with this position in a real-world environment, it must be understood that the CPP cannot, and should not, partake in activities or conduct that allows the CPP to not be tactically ready in the event of an attack (Dale 2008).

Site Advance

Conducting a comprehensive and effective site advance is a term used to ensure the location the celebrity will visit is safe; and the necessary security precautions and planning have been conducted. Site advance is a critical part of close protection security and will encompass many areas, activities, and locations the celebrity will visit. Arriving at a location prior to the celebrity will ensure that the location is safe, as well as secured to prevent an attack or incident from occurring. This important responsibility can help in preventing harm or even embarrass to the celebrity. The advance person must survey the location for dangerous conditions that could affect the safety of the celebrity and the security team. The CPP must also coordinate with the host committee representatives to confirm and verify the specific activities that will take place when the celebrity arrives.

The CPP should request support from security and engineering staff at the location to help with identifying a primary and secondary access point, internal and external threat information for the location, infrastructure concerns, and any other important information relating to the location that could affect the security and safety of the celebrity. The site advance should evaluate the exterior for large crowds, paparazzi, unusual behavior, or dangerous conditions. The arrival area should be clear and metal barriers used to "contain" the crowd and paparazzi so the celebrity is not surrounded upon exiting their motorcade. Large uncontrolled crowds can restrict the movement of the celebrity and the security team, as well as increase the risk of injury to the celebrity. If the crowd or paparazzi will not adhere and remain behind the barriers, the CPP should consider, not removing the celebrity from the motorcade, using a secondary arrival location away from the crowd or depart the area all together. The same applies for a departure, which many times will occur when the public is alerted that a celebrity is present at a location and they are now staged in front. If the crowd becomes too overwhelming, the police should be requested for crowd control and alternate departure plans considered to avoid direct interaction with the crowd. The primary reason for avoiding the crowd is the protection of the celebrity and the CPP (Dale 2008).

Countersurveillance

Countersurveillance for the celebrity can be difficult as the celebrity is usually surrounded by fans and curiosity seekers. The CPP most likely will encounter overzealous fans and possible stalkers. A potential threat must be identified and precautions taken to ensure the safety of the celebrity. A comprehensive close protection security plan must include effective and robust countersurveillance strategies. The ability of the CPP to identify potential attackers must be a priority of the CPP. When threatening or harassing information is received, the CPP must conduct a thorough investigation to ensure all information regarding the individual or group is known; so any security enhancements, if needed, are conducted. Protection intelligence requires gathering information, including any threatening communications against the celebrity toward developing a comprehensive background of the person. This should include a description of the person, any background information, such as mental illness, criminal history, and access to weapons and if they are prone to violence. A recent color photo should be obtained and shared with the celebrity, their staff, and the entire CPP team of the celebrity. The information should be continuously updated, analyzed, and used to direct the necessary security changes toward addressing the threat and reducing any risks. Threats made to the celebrity should be forwarded to law enforcement for investigation and, if necessary, possible arrest. It is important that the CPP advise the celebrity of the seriousness of following all security recommendations to ensure the highest level of safety and security (Dale 2008; USDS 1998).

First Aid

Administrating first aid must also be part of the celebrity protection plan. Providing immediate

medical treatment in the event of an attack, medical condition, or accident is the responsibility of the CPP. First aid planning and training must include CPR, providing direct pressure for trauma injuries and being aware of medical conditions of the celebrity. The CPP should be certified in first aid, and certification should be renewed every year. The CPP should be familiar with area hospitals and include in the motorcade route plans the names and addresses and if it is a Level 1 trauma center. The CPP should be familiar with any medicines or medical conditions the celebrity has to advise emergency room physicians when needed (Oatman 2006).

Threat Assessment Analysis

A threat assessment has become a valuable tool in the close protection field. Many governmental agencies and private security firms use this important tool in calculating risk. Here we learn the importance of using a threat assessment to identify potential dangers that the celebrity may encounter. When tasked with developing a threat assessment on the celebrity, the CPP must gather as much information as possible on the person (s) who may have an interest, motive, intention, and, more importantly, the capability of mounting an attack. Gauging the possibility of a potential attack is critical to the protection of the celebrity and the CPP (Fein and Vossekuil 2000). The information must include all data and other sources of information pertaining to the celebrity and his or her family. Open-source information, known threatening communications, and paid intelligence services can all help in calculating a comprehensive threat assessment. Known threateners should be investigated and a records check conducted to include criminal history, mental health, community relations, and social services. Individual motives related to the behavior of a potential attacker also play a role in the overall threat assessment process. Unfortunately, there is no one descriptive profile of an attacker. Assassins come in many shapes, sizes, intelligence, and other characteristics. However, an attacker will engage in familiar behaviors and actions before they attack.

When a person decides to mount an attack on a target, a number of preparatory steps must be taken. These steps have visual characteristics that can be observed by the CPP. These steps would most likely include acquiring a weapon, surveying security near the celebrity, and the development of an attack and escape plan. A misconception the CPP can make is to analyze threatening information based on a *presumption* that a potential attacker is always mentally ill. Research on known threateners has disclosed only a small percentage is actually emotionally disturbed. On the contrary, most attackers chose assassination because it afforded them a way of achieving a goal or to solve a problem. Additionally, another myth of a potential attacker is that a threat is made prior to the attack. Though many have written letters or made threatening telephone calls, the majority of assassins were not known or anticipated because they were anonymous until the day they decided to attack (Fein and Vossekuil 2000).

Close Protection Terminology

Close protection security uses specific terminology to ensure confidentiality and operational security for the celebrity, their family, and the security team. Exposing specific addresses, names, and activities can be very detrimental to the celebrity and the CPP, as it can alert a potential attacker where the celebrity is located, the time of arrival, the location, and what activity will take place when the celebrity arrives. The CPP should utilize "code words" that are changed regularly to ensure that any stalkers, criminals, hackers, or potential attackers cannot obtain sensitive information that could help in executing a successful attack on the celebrity. These code words can be used for residences, scheduled locations and activities, as well as motorcade movements on a secured route. The use of checkpoints, which are described over a security team communication radio, can alert the entire security team of where the celebrity is in relation to the site and within the motorcade route (Holder and Hawley 1998).

Attack on the Principal: AOP

It is likely that the celebrity may at some point be the target of an attack, whether by gun, knife, or even a whipped cream pie. Either way, if the celebrity is attacked, the CPP has failed. The CPP's ability to perceive and identify danger will be in question, and retraining will be needed. Tactics are available that many CPP use to combat a threat, but constant vigilance and attitude are equally important. One primary tactic used is known as the "arm's reach" method. The arm's reach method means the CPP is always at "arm's reach" from the celebrity so the CPP can move them from the danger zone when needed. Firstly, awareness by the CPP that a gun or other weapon has been produced in the presence of the celebrity is critical. The CPP must now act instantaneously and "sound off," "cover," and "evacuate." If the attack is from an object that is thrown, i.e., a brick, an egg, or a liquid, the "arm's reach" method is used to remove the celebrity to a safe area or location, such as a room or the motorcade. If the incident is found only to be a thrown egg and no immediate threat of injury is present, the CPP can allow the celebrity to return to the area where the incident occurred, if deemed to be safe. The use of the "clock method" to identify the location of a threat is an effective way to determine where the threat is in relation to the celebrity and the CPP. This successful tactic uses the 12 o'clock position, which consists of identifying a fixed object on a wall or location. If an attack or weapon is produced, the CPP using the clock method should identify the threat from its position in the clock. For example, if someone produces a knife at the 3 o'clock position, the CPP should *cover and evacuate* the celebrity toward the 12, 6, or 9 o'clock position if possible. The concept is to remove the celebrity from the threat and out of the immediate danger zone (USDS 1998).

Close Protection Formations

Each situation is determined by environmental circumstances that will either allow or disallow a CPP to make certain adjustments to a formation. Alternate and contingency plans should also be prepared to cover such circumstances, as weather, threats, or any other actions that may affect the security of the celebrity. Security planning is the responsibility of the CPP working with the celebrity. The protective security team should remain close to the celebrity at all times, because the overall objective is to protect the celebrity from harm and/or embarrassment. Protecting the celebrity will require utilizing effective protective formations, which can be used in certain circumstances. The formations being discussed are all part of a holistic and effective close protection security strategy to ensure that security personnel are placed strategically around the person being protected. Protective formations are all part of a structured security environment that can help circumvent any attempt from someone attempting possible harm. It must be stated that protective formations are not an absolute; however, it can help in ensuring security is placed around the celebrity to lower the risk. The following formations are used in close protection security today and have proven to be an effective and resilient tool in the overall security plan.

Lone formation utilizes *one security person* with the celebrity and can be used in both internal and external movements. The lone formation requires the CPP to stand behind the celebrity at an angle and not directly behind for better field of view and observation. Known as the number one, this person is responsible for removing the celebrity from the area when required. In order for the number one to be effective, the CPP must maintain an *arm's reach* from the celebrity at all times in the event of an attack. It is important that the CPP remain vigilant and maintain the "arm's reach" behind the celebrity at all times. Unfortunately, this is not always possible because of reluctance of the celebrity to allow the CPP to be so close. However, allowing too much distance (more than arm's reach) between the celebrity and the CPP can result in injury if the person cannot be removed from a dangerous environment quickly (Dale 2008).

Another formation utilized is known as the *slash or sweep formation*, which requires an *advance person* to lead the protective formation. This formation requires a *two-person security team*: one as the advance, who knows exactly

where the team must go, and the number one who is responsible for the safety and security of the celebrity. However, human nature will play a role in how the protective formation is effective when dealing with an attack. Instinct and human reaction many times cause individuals to engage an attacker when their responsibility may have been to the celebrity. Another formation is known as the *wedge formation*, which will require more security personnel and should be used when a higher threat level has been assessed for the celebrity. The use of an advance person, a number one behind the celebrity and another CPP positioned on the opposite side of the number one, can enhance the overall security environment. This formation is used in public settings where access by the public is possible.

Close Protection Motorcades and Route Management

A major part of the close protection security plan is the development of a robust transportation safety structure. Motorcade and route management is a primary security mechanism for the celebrity's security plan. Ensuring that the celebrity and the security team remain safe will require strategic and critical thinking skills that anticipate danger and ensure the CPP can respond quickly and effectively in the event of an attack. Motorcades can range from one or more vehicles; and though motorcade sizes may vary, the fundamentals remain the same. Vehicle transportation is considered vulnerable, because the CPP team is not in a strategic and ready position. Individuals attempting to photograph or even harm the celebrity can easily approach the motorcade. This is a dangerous scenario and is up to the CPP team to remain vigilant and anticipate any and all threats that can occur. Motorcade planning must ensure that the CPP is trained in evasive driving techniques. There are various independent and accredited schools that can train the CPP in evasive driving techniques throughout the country. The CPP driver must operate the vehicle in a safe and responsible manner at all times and only when under attack should the operator make any evasive moves.

The celebrity is the primary asset in a motorcade and whatever vehicle the celebrity is situated in the vehicle will be identified as the limo. The celebrity should be situated in the right rear of the limo, as this is done for onside arrivals. The CPP must develop secured routes when transporting the celebrity in the motorcade. The first designated route is known as the *primary route*, followed by a *secondary route*, and in certain circumstances, a *tertiary route* may be designated. Multiple routes are needed in the event of threatening information, an attack, hostile surveillance, or a traffic condition. The CPP must observe all road and environmental conditions and potential problems on a particular route. Challenges and potential threats include construction, traffic congestion, demonstrations, roadway chock points, as well as weather and pavement condition. These are just a few of the concerns the CPP must anticipate, assess, and calculate when developing motorcade routes (Dale 2008). The routes should be determined based on safety but also the ability to evacuate and retreat in the event of an attack. Safe locations or *safe havens* on the route would include police stations, fire stations, hospitals, government buildings, and even corporate locations that have security positioned in the lobby.

Motorcade Alignment and Vehicle Positioning

The positioning of the motorcade vehicles is critically important and part of a strategic design platform in close protection security. The theory of aligning cars is part of a security environment that does not expose the celebrity unnecessarily and provides tactical positioning for the CPP. After the vehicles have been inspected and secured, they are now ready for alignment and positioning. A motorcade configuration should include a lead car to pilot the motorcade. The lead car will know the motorcade routes and act as an advance toward identifying hostile surveillance or a dangerous condition that may affect the motorcade's movement. The second vehicle in the alignment is known as the limo, which was previously discussed. The third vehicle in the

motorcade is known as the follow vehicle, which will have additional security personnel who are part of the protection team. They will form a protective formation around the celebrity once he or she exits the motorcade. This is known as a secured package, and it is also utilized in many diplomatic and executive protection security details. The vehicles should be the same make, model, and color to avoid an attacker or paparazzi from easily identifying the vehicle carrying the celebrity.

The positioning of the motorcade with the limo in the center also allows the follow vehicle to become a replacement vehicle for the celebrity in the event that the limo was to become disabled. Strategies such as these have been very effective in maintaining a high standard of security for the all types of close protection security. Motorcade movement is a critical part of the security plan as the celebrity may decide to walk or jog on occasion. The motorcade must shadow the celebrity during these moves. Though this is not always possible, the security team should ensure that routes are determined if possible prior to any walking moves. Routes for the celebrity when walking should be with the flow of r so the motorcade can proceed and continue to shadow at a close distance. Counterflow is not recommended as it will cause the motorcade to reposition away from the celebrity, which increases the overall risk exposure in the event of an incident or attack (Dale 2008).

Physical Security Concepts and Residential Security

The CPP team will also be responsible for surveying and installing physical security measures around the celebrity's residence. Since many attacks, especially kidnapping attempts, occur at a person's residence, providing productive and effective security protection measures will be a necessary component of the close protection plan. Implementing physical barriers, such as fencing and motion sensor lighting, will protect the perimeter from a possible intruder. CCTV surveillance cameras should also be installed, which the CPP, as well as the celebrity, can view the property both remotely and while inside the residence. Additional security measures include a grade 1 or 2 locking mechanism, solid wood doors on the exterior of the residence, as well as anti-shattering window filming. Interior rooms of the residence should have intrusion detection sensors on windows and doors, glass break detection, and life safety equipment such as CO2 and smoke detection. Panic room consideration should also be part of the security survey, and rooms within the residence should be identified as potential panic rooms (USDS 1998).

Attire and Equipment

The CPP must wear appropriate attire that is conducive to the professional environment they are working in. Like training, professionalism, and attitude, having the proper equipment and presenting an assertive look are important in the overall protection of the celebrity. This section will describe the equipment needed for the CPP and the clothes that should be worn. When assigned to the protective security detail, the member needs to obtain certain equipment that will assist in the protection of the celebrity. Protection equipment will vary from team to team and from environment to environment. Individuals may feel the need to equip themselves with the necessary items that will do the job at hand. As a member of the security team, you are on the front lines, not only in regard to an attack, but in the public's eye. The message sent will have an impact on the celebrity and the entire team. Personal appearance is as important as training, and both need to be followed and practiced on a continuous basis. The following is a guide on the proper dress code for a member of the security team:

Males and Females

- Single-breasted, dark blue, black, or dark gray suits are preferable
- Dark-colored sport coat and slacks can also be worn
- White or light blue shirts with simple color ties
- Slip-on shoes, rubber sole, preferably black
- Golf shirt with khakis, only under nonbusiness occasions

Equipment

Communications
- Radio with surveillance kit (earpiece)
- Radio holder, pager (if needed)
- Cellular telephone. Smartphone technology is recommended

Flashlight
- Compact flashlight with extra batteries
- Writing note pad
- Working black ink pen
- Firearm (if authorized) with belt holster and extra magazine clip. Carry permit and other identification for law enforcement purposes

References

Dale, J. (2008). *Introduction to executive protection* (2nd ed.). Boca Raton: CRC Press.

Fein, R., & Vossekuil, B. (2000). *Protective intelligence and threat assessment investigations*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Holder, P. T., & Hawley, D. L. (1998). *The executive protection professional's manual*. Boston: Butterworth-Heinemann.

Oatman, R. (2006). *Executive protection. New solutions for a new era*. New York: Noble House.

United States Department of State: Protection Training Manual. (1998). USDS.

Corporate Security

Kevin A. Cassidy
Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Corporate security · Crime prevention · Environmental design · Ethics and compliance · Workplace violence · Collective bargaining agreement · Electronic security systems · Design basis threat · Classical persuasion model – CARVER

Definition

Corporate security is responsible for overseeing the physical protection of a company's property, personnel, data, and intellectual assets, as well as identifying, mitigating, and managing security and safety threats to the company's resilience and continuation.

Introduction

Corporate Security focuses on the application of governance practices to ensure company principles, polices, and procedures are identified and applied as designated within the organization. Two major changes in corporate security since September 11, 2001, include the types of people who serve as directors and the policies implemented (Nemeth 2018). Initially, the majority of security directors had been retired law enforcement officers who worked predominantly in inner cities, trying to reduce crime and assist the public. Corporate America's mentality was that retired law enforcement officers would be good directors because they had the experience and expertise in dealing with security and criminal matters (Nemeth 2018). Organizations today are seeking security professionals with former military experience or law enforcement backgrounds, as well as an advanced degree in business, security, or management (McCrie 2016). These directors need to know about both public and private security notions, including: community policing, crime prevention through environmental design, electronic access control and monitoring systems, loss prevention, protection of intellectual property, how to deal with active shooters, and implementing emergency management (Nemeth 2018).

Changes in corporate security's policies occurred as a result of its global function in today's society. The security management team is responsible for surveying, mitigating, and managing an organization's footprint (McCrie 2016; Nemeth 2018). It ensures the continuance of an organization when a disaster strikes through planning and strategy development. Any potential

Corporate Security, Fig. 1 12 Organization's strategies

Budgetary Management	Business Continuity	Crime Prevention Through Environmental Design (CPTED)	Emergency Management
Ethics and Compliance	External networking	Health and Safety	Internal networking
Investigations	IT Security	Physical Security	Workplace Violence Programs

threat must be considered and reviewed by security personnel (McCrie 2016). The team must also take into consideration that not all strategies will fit an organization's security profile (see Fig. 1). For example, security procedures from hospitals, retail stores, and education facilities will be significantly different. Organizations must adhere to security regulations and standards based on their city, state, and federal classifications, as well as the industries' governing bodies.

Corporate Security continues to face challenges as corporations expand and increase their profits, requiring private security to protect its assets (McCrie 2016). Many organizations are now hiring Chief Security Officers (CSO). The CSO is an organization's most senior executive accountable for the development and oversight of policies and programs (The Hallcrest Report II). The CSO is part of the C-Suite (i.e., titles beginning with "chief") which is usually the most senior executives in the organization (e.g., Chief Executive Officer, Chief Marketing Officer, Chief Financial Officer).

Chief Security Officer

The CSO is responsible for the protection of life and property of all those working at or visiting the company's facilities. The main duties of the CSO is to forge interdepartmental connections (e.g., Facilities, IT, Legal, Communications, Human Resources and Procurement) and to develop policies and strategies that safeguard and protect all assets owned by the organization. It is important for the CSO to stay current regarding all internal and external security and safety related issues. The CSO must ensure the security staff are properly trained and equipped to deal with potential issues that arise and mitigate these hazards as quickly as possible (see ▶ "Personnel Security: Training" in this encyclopedia). CSOs manage all investigations and formulate strategies to respond to serious events that may impact the organization. Events, such as labor disputes, weather conditions, power disruptions, terrorism, and active shooter incidents, can impact an organization on multiple levels. Their ability to interface with external organizations, from law enforcement agencies to local community groups, is vital to their success, as is their ability to understand accounting and budgeting responsibilities. Finally, CSOs must be able to communicate their visions to the organization effectively.

Challenges for Corporate Security Department

So, what exactly are the challenges of Corporate Security department? In this section, the six challenges that corporate security departments face (i.e., Budgets, Electronic Security Systems, Workplace Violence including Active Shootings, Fire Safety, Communications and interfacing with External Agencies) are discussed.

Security Budgets

The Chief Security Officer is first tasked with creating and maintaining a budget in efficient and effective manner (Harrison 2014). Large organizations have security in the hundreds of thousands or millions of dollars. The Corporate Security executive must interface with senior management and finance departments to ensure the security budget remains on track for the company's calendar (i.e., January 1 to December 31) or fiscal (i.e., covering 12 consecutive months, but starting in any month) year.

Two factors that security departments take into consideration are direct labor costs and operating budgets. Direct labor costs are factored by the number of employees you have within your department and the benefits you provide for them. If employees in your organization belong to a labor union, many of the costs and pay raises are covered under the collective bargaining agreement (CBA). An operating budget is a financial document that illustrates funds needed to keep the security department operating effectively. Items can range from training, to ESS, uniforms and supplies, just to name a few.

Electronic Security Systems (ESS)

The second challenge for security departments is the understanding and utilization of Electronic Security Systems (EES) your organization employs. This can include the following: CCTV's, Access Control Systems, Mail Room Detection Systems, Glass Break Detection, Electronic Eavesdropping Detection Equipment, and IT Monitoring Equipment. In many organizations, the IT department will have its own budget to protect the corporation's data and electronic files. However, when a system is breached, Corporate Security may become involved in the investigatory process working alongside the IT department (see ▶ "Investigations: Criminal" in this encyclopedia). There are a few reasons for purchasing an ESS system. The first is to protect life and property. The second is to utilize the equipment with personnel to respond to incidents faster. The third is to create systems that can track and monitor internal and external movements of personnel, visitors, and guests to ensure their safety.

Three factors must be considered when a company purchases any type of Electronic Security Systems. First, the individual responsible for the purchasing of the equipment must decide how the ESS will enhance the organizations operability. The decision will be based on whether a site survey had been conducted and regulatory requirements had been reviewed as justification to add or enhance current ESS. Specifically, the company should survey to determine what advantages the ESS component will afford a company, as well as its costs. For example, an organization seeking to add another closed-circuit television system to an existing system would need to ensure that the monitor(s) is capable of adding an additional camera(s), the length of the cable or wire run to connect the device is configured appropriately, and the correct camera is selected, such as a pan-tilt-zoom (PTZ) or stationary camera, and whether it is functional in low light conditions.

Second, the company must consider the cost associated with the purchase of an ESS. The costs can vary from product to product. It is imperative that a security professional with experience in designing and installing security systems be involved. In determining which vendor to select, it is advantageous to obtain three bidders and always write the Request for Proposals (RFP) for the bidders with two necessary components in mind. Next, conduct a Request for Information (RFI) on each company selected to submit proposals on the ESS project. The RFI is a document used to obtain information about the company which can include their products, services, or suppliers. In many large organizations, the purchasing or procurement department will assist you in undertaking this task. Finally, advise the bidders that the specific camera, monitor, door alarm, panic alarm, and housings to enclose these devices must be used. This requirement will force the bidders to submit proposals using only the requested products and materials. The price difference should be in the labor costs only, which allows an organization to conduct a comparative cost analysis.

Third, the company must develop an oversite group who will be responsible for writing policies and procedures. Determine what the primary purpose would be for installing the ESS system, that is, its specific intention. A policy needs to be written outlining the functionality of the specific ESS. For example, the best performance would be to interface the CCTV's with an alarm monitor so that when an alarm is activated, the closest CCTV(s) to that activated device should appear instantly on the alarm monitor. This allows the individual monitoring the system to observe in real time what has just happened. Procedures need to be developed instructing the operators what to do in the event of a crisis. These procedures should be reviewed after each incident or at least on a monthly basis (see ▶ "Physical Security: Exterior Application" in this encyclopedia).

Workplace Violence and Active Shooters

The third challenge is workplace violence (e.g., hostile workplace, bulling or cyber bulling, stalking, sexual harassment), with emphasis placed on active shooter training (see ▶ "Workplace Violence: Active Shooter/Terrorist Threats" in this encyclopedia). In 2016, there were 500 homicides in the workplace and 394 of those victims were intentionally shot and killed (Strom et al. 2010). Additionally, a total of 792 injuries were intentionally inflicted on workers, an increase from 646 the year before in 2015 (Caine 2018; see ▶ "Workplace Violence: Assault" in this encyclopedia). Corporate Security departments have become involved in mitigating various incidents, especially when it involves co-workers (Lindell et al. 2015). In most incidents, there is a three-pronged approach to these investigations. Usually Human Resources receives the complaint and investigates it themselves or involves Corporate Security and/or Legal (Sylves 2015). Depending what the corporate policy is, the investigation can proceed in one of many directions. At times when a victim thinks the claim was not adequately investigated, the employee will go to local law enforcement or the media. When this occurs, it is imperative to involve the organization's communications department. All inquiries should be directed to them, and other departments should be advised not to discuss the case and refer all questions to the Communications Department.

A recent report by the FBI (Silver et al. 2018) examining active shooter cases from 2000 to 2013, provided information useful in understanding the preattack factors that contributed to these incidents in which multiple people were injured and killed with firearms and bombs. All businesses will need both active shooter awareness and mitigation training (Interagency Security Committee 2015; Wallace and Webber 2018). The main information provided included that has been an increase over the past 7 years in active shooter incidents, incidents occurred predominantly in commercial settings, the majority of shooters were lone men, and that more than half of the shootings ended by the shooter either fleeing or committing suicide, particularly after law enforcement engaged with the shooter (Silver et al. 2018).

Many organizations are training their staff on how to deal with an active shooter situation. They are interfacing with local law enforcement agencies and hiring external consultants to train their staff on recommended guidelines to follow during an active shooter situation (see ▶ "Public-Private Partnerships: Training and Coordination in Disasters" in this encyclopedia). Depending on your business and your building active shooter plans will vary from location to location. The three primary objectives law enforcement communicate to the public during mitigation training are: "Run-Hide-Fight." If possible, run from the active shooter safely. If running is not an option, hide from the shooter. Once inside a secured area, lock the doors, turn off the lights, call "911" if possible and silence your cell phones. The last alternative is to grab any item in the area and use it to defend yourself and fight back against the shooter.

Corporate security must "harden" their company to prevent becoming a target. One method to do this is called Design Basis Threat (DBT) which aids in reducing or mitigating risk by implementing physical security barriers or ESS. DBT is a basis for designing systems to

protect against acts of aggression against an individual or organization. Examples include placing bollards around the perimeter of your facility to stop or deter a vehicle from crashing into your building, or ensuring all individuals entering your location have an updated access control card or visitor's badge so former disgruntled employees or visitors who attempt to re-enter the facility will be intercepted (see ▶ "Physical Security: Exterior Application" in this encyclopedia).

Fire Safety

The fourth challenge is fire safety and laws vary by jurisdiction. In many locations, their security officers act as Fire Safety Directors, Assistant Directors, Floor Wardens, Floor Searchers and Aiding the Disabled to name a few other responsibilities (see ▶ "Fire: Prevention, Protection, and Life Safety"). Corporate security departments will need to interface with facility or building managers to become familiar with the fire codes and ordinances. Within the United States, many organizations comply with the National Fire Protection Association (NFPA). The NFPA creates and maintains private, copyrighted standards and codes for usage and adoption by local governments. The NFPA works to achieve these goals by delivering information and knowledge through their more than 300 codes and standards, research, training, education, outreach, and advocacy and by partnering with others who share a similar vision and an interest in furthering their mission.

Communications

The fifth challenge is communications. Every organization thinks it is prepared for communicating during a crisis, but unfortunately, they may not be. In most instances, corporate security is one of the first departments to learn of a crisis and then it often fails to enact the communication protocol. The Communications Department/Media Information Department can be a significant partner if utilized properly. It is imperative to formulate a crisis communication team to ensure that one strong, accurate message will be sent in a timely manner notifying all stakeholders of the status before, during, and after the crisis (Lindell et al. 2006). It is also necessary to appoint one spokesperson for your organization. This individual should be part of the communications team and will be designated point person to answer all questions and inquires.

Global security departments should consult a communication specialist for every location in which their organization is located. The message will be designed consistent with the type of business it is, the stakeholders it has, and legal requirements. In the last 2 years, misinformation on social media and "fake news" have become a concern for businesses. It is important that any incident affecting the company is communicated to the public accurately particularly as individuals are able to upload and distribute information at the tap of various communication devices. Once information is out there, it is thought to be factual. It is advantageous for an organization to inform the stakeholders of the issue(s) in a proactive manner rather than stakeholders and employees seeing it first via social media.

Interfacing with External Agencies

The sixth challenge for corporate security departments is interfacing and sharing information with other city, state, federal, global, and private organizations. The CSO must become familiar with a variety of external agencies and be able to define both risks and threats to the company depending on its size, goals, structure, and business model (Nemeth 2018). To do this, the Security Professional can use the CARVER System, an acronym that represents the following attributes – criticality, accessibility, recuperabiilty, vulnerability, effective, and recognizable.

The first step is to measure public health and economic impacts of an attack (Lindell et al. 2006). For example, what would happen to your employees or organization if a medical crisis affected your organization (e.g., rubella outbreak, Severe Acute Respiratory Syndrome/SARS that occurred in 2004). The second step is the ability to access and egress from a target physically. Accessibility is the directness of the target to the threat so the CSO must consider whether the organization has created a plan to mitigate or reduce the

threat of an attack. The third step is the ability of a system to recover from an attack (Wallace and Webber 2018). The CSO should determine how quickly the organization can be operational after a crisis (see ▶ "Business Continuity Plan" in this encyclopedia). The recovery time objective (RTO) is the maximum tolerable length of time that a computer, system, network, or application can be down after a failure or disaster occurs. The fourth step involves the ease of accomplishing attack against the company. By conducting a Strength, Weakness, Opportunity, and Threat (SWOT) analysis, organizations can determine how vulnerable they are to both external and internal threats. The fifth step involves the amount of direct loss from an attack as measured by loss in production. Organizations must equate how lost revenue and reputation may affect the bottom line. In particular, the CSO must determine when a crisis occurs, what the RTO is before a company can recover from a crisis. The sixth step is the ease of identifying the target. Organizations need to focus on how the degree to which specific building, system, or network is relaxed. Once an analysis is conducted, countermeasures must be incorporated. Corporate security must conduct an author or hire an external security consulting organization to do so. Once the CARVER method is applied, it is imperative for the Security Director to reach out to other security professionals within the field, as well as to the various public sectors including city, state, and federal organizations, in order to network and share information regarding how to enhance security on a domestic and international scale.

Conclusion

Corporate security will continue to face internal and external challenges. A paradigm shift in security has occurred due to the introduction of new technology, methods, and trends in response to threats and criminal actions against corporations. As quickly as a threat is discovered in business, it is the responsibility of the corporate security department to mitigate it. This takes strategy, financing, and support from senior management to mitigate risks and operate an effective corporate security department.

Cross-References

- ▶ Business Continuity Plan
- ▶ Emergency Management: Evacuations
- ▶ Fire: Prevention, Protection, and Life Safety
- ▶ Investigations: Criminal
- ▶ Physical Security: Exterior Application
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Protection and Security in Public Spaces
- ▶ Public-Private Partnerships: Training and Coordination in Disasters
- ▶ Workplace Violence: Active Shooter/Terrorist Threats
- ▶ Workplace Violence: Assault

References

Caine, A. (2018). In response to office violence. *Business Insider*. Accessed at https://www.businessinsider.com/shooting-drills-at-work-2018-4

Harrison, R. (2014). Managing and defending a security budget. In R. Harrison (ed.), *Security leader insights for effective management* (pp. 57–61). Amsterdam: Elsevier Inc.

Interagency Security Committee (2015). *Planning and response to an active shooter: An interagency security committee policy and best practices guide*. Accessed at https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf

Lindell, M.K., Prater, C.S., & Perry, R.W. (2006). Fundamentals of emergency management. Accessed at https://training.fema.gov/hiedu/aemrc/booksdownload/fem/

McCrie, R. (2016). *Security operations management* (3rd ed.). Waltham: Butterworth-Heinemann.

Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.

Silver, J., Simons, A., & Craun, S. (2018). A study of the pre-attack behaviors of active shooters in the United States between 2000–2013. Federal Bureau of Investigation, U.S. Department of Justice, Washington, DC. 20535.

Sylves, R. (2015). *Disaster policy & politics* (2nd ed.). Thousand Oaks: Sage.

Strom, K., Berzofsky, M., Shook-Sa, B., Barrick, K., Daye, C., Horstmann, N., & Kinsey, S. (2010). The private

security industry: A review of the definitions, available data sources, and paths moving forward (NCJ No. 232781). Retrieved from National Criminal Justice Reference Service website https://www.ncjrs.gov/app/publications/abstract.aspx?ID=254874

Wallace, M., & Webber, L. (2018). *The disaster recovery handbook* (3rd ed.). New York: Amacom.

Further Reading

Doss, K. T., & Shepherd, C. D. (2015). *Active shooter-preparing for and responding to a growing threat*. Oxford: Elsevier Inc.

Huehls, R., & Lackey, Z. (2018). *Building a modern security program*. O'Reilly Media Inc. Accessed at https://www.oreilly.com/library/view/building-a-modern/9781492044680/

Maras, M-H. (2016). *Cybercriminology*. Oxford: Oxford University Press.

Thompson, G. J., & Jenkins, J. B. (2013). *Verbal judo: The gentle art of persuasion*. NY: Harper Collins Publishers.

Criminals: Active Shooters

Kevin A. Cassidy
Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Bullying · Domestic abuse · Workplace violence · Proactive · Reactive · Training

Definition

According to the Department of Homeland Security (DHS 2008), an active shooter is a person "actively engaged in killing or attempting to kill people in a confined and populated area" (DHS 2017 p. 2). This individual is aggressively involved in killing or attempting to kill people in an occupied location.

Introduction

There is a plethora of information on emergency response to active shooters available through various federal, state, and local agencies. Statistics provided by these agencies help us understand various information from each shooting including age, sex, demographics, social economics, the type of weapon used, and the venue of the shooting in an effort to correlate factors trying to understand comparisons or reasons if any.

In a typical active shooter scenario, people are in the process of their daily lives, perhaps sitting at a desk, in an open area like a classroom or hospital waiting area. All of a sudden, the sound of gunfire erupts. Most people's adrenaline will increase and the flight vs fight response activates. What should people do in this scenario? Experts in law enforcement discuss two methodologies you can incorporate to save yourself. First is the "run–hide–fight" technique, and the second is the ALICE technique which means "alert, lockdown, inform, counter, evacuate." Deciding which method is best for you depends upon your location and your familiarity of the location where you are at the time.

The scope of this paper is threefold. First, the chapter will provide an overview of what can be expected after a shooting, as well as how individuals; businesses; federal, state, and city agencies; and the media react to these events. Second, the chapter will describe the types of challenges faced by the agencies, communities, and families involved and the public as well. Third, the chapter will propose ideas of what needs to be done to move forward.

Run, Hide, Fight

Individuals caught in an active shooter situation need to resort to whatever action they find the most appropriate for their circumstance. The "run–hide–fight" method is what the DHS (2008, 2017) recommends to the general public. The actions you take to survive are based on what you are seeing and hearing at the time. "Run–hide–fight" is one way of trying to remove yourself from where the shooting is taking place. If possible, escape by running. "Run" in the opposite direction of where you are hearing the sound of gunfire. Leave the building or area by running as far as possible from where you heard the shooting. Sometimes you may have to run to a location within the

building that is deemed safe. If you are unfamiliar with the building, follow the other occupants who are running as well. Don't assume someone else has phoned "911." Once you are in a safe location, notify "911" and advise them of the situation (Burke 2000).

The advice is to "hide," if you are unable to exit the facility, for whatever reason. Find a location out of the shooter's view and lock the door if possible. If locking the door is not an option, block the door with whatever furniture or materials you have at your disposal. Once it is safe to do so, notify "911" and advise them of your location. Turn off all lights, close the blinds to windows or doors if possible and place your phone on vibrate. You should never leave a secured area until law enforcement officers have arrived and properly identified themselves (Burke 2000).

If you are not able to run or hide, then your only option is to "fight," that is, if confronted by the shooter, "fight" aggressively as possible to disarm the shooter. Using anything at your disposal, including a fire extinguisher, garbage can, chair, or desk, and be prepared to end the attack by causing injury or death to the shooter. If others are available or hiding nearby and it is possible, work in teams to protect your safety.

ALICE

As referenced by the ALICE Training Institute in Medina, Ohio, they break down the methodology behind the ALICE acronym. "A" stands for Alert. Alert is when you first become aware of a threat. The sooner you understand that you're in danger, the sooner you can save yourself. A speedy response is critical. Seconds count.

Alert is overcoming denial, recognizing the signs of danger and receiving notifications about the danger from others. Alerts should be accepted, taken seriously, and should help you make survival decisions based on your circumstances.

"L" stands for lockdown. If evacuation is not a safe option, barricade entry points into your room in an effort to create a semi-secure starting point.

Our training explains scenarios where lockdown may be the preferable option and dispels myths about passive, traditional "lockdown-only" procedures that create readily identifiable targets and make a shooter's mission easier. ALICE trainers instruct on practical techniques for how to better barricade a room, what to do with mobile and electronic devices, how and when to communicate with police, and how to use your time in lockdown to prepare to use other strategies (i.e., counter or evacuate) that might come into play should the active shooter gain entry.

"I" stand for inform. The purpose of inform is to continue to communicate information in as real time as possible, if it is safe to do so. Armed intruder situations are unpredictable and evolve quickly, which means that ongoing, real-time information is key to making effective survival decisions. Information should always be clear, direct, and in plain language, not using codes. If the shooter is known to be in an isolated section of a building, occupants in other wards can safely evacuate, while those in direct danger can perform enhanced lockdown and prepare to counter.

"C" stands for counter. ALICE Training does not believe that actively confronting a violent intruder is the best method for ensuring the safety of those involved. Counter is a strategy of last resort. Counter focuses on actions that create noise, movement, distance, and distraction with the intent of reducing the shooter's ability to shoot accurately. Creating a dynamic environment decreases the shooter's chance of hitting a target and can provide the precious seconds needed in order to evacuate.

"E" stands for evacuate. Evacuating to a safe area takes people out of harm's way and hopefully prevents civilians from having to come into any contact with the shooter.

Did you know that you should break a window from the top corner as opposed to the center? Many useful techniques that civilians do not know exist and can save your life.

After an Active Shooter Incident

There will be many challenges faced by a company after an active shooter incident. The emotional and physical toll it can have on personnel

may last a long time. The effects of post-traumatic stress disorder will vary for each individual, and companies must be prepared to deal with these issues at multiple levels from employees to supervisors, individually, and in groups (APA 2019). Security and law enforcement agencies will need to reassess physical security measures. Each department in the company will need to update their business continuity plans, and human resources will need to develop strategies along with senior management to move the company forward. There are many factors to consider after an active shooter incident. There are three key factors that are essential to the continuance of a company: emotional support; human resources' challenges and goals; and business continuity.

Emotional Support

According to the American Psychological Association (2019), "We do know, though, that it is typical for people to experience a variety of emotions following such a traumatic event. These feelings can include shock, sorrow, numbness, fear, anger, disillusionment, grief and others. You may find that you have trouble sleeping, concentrating, eating or remembering even simple tasks" (para 2). It is imperative for companies to offer counseling or workshops for employees and their families and friends who have been through a traumatic event. Also, for businesses, town hall meeting is another way to advise employees what management is doing and for questions to be addressed.

According to the DHS (2017) "Recovery is a continuous process that occurs over short- and long-term incremental phases. Organizations and their staff will progress through the recovery phase at a different rate, and each will require varying degrees of assistance" (p. 1).

Human Resources Department: Challenges and Goals

Senior management needs to meet with the leaders of the human resources department to discuss and review the company's Employee Assistance Program (EAP). Human resources must focus on short-term goals and long-term goals. The short-term goals are crafted to ensure employees receive the proper medical and psychological care they require. An information hotline should be established so employees and family members can obtain medical information regarding any questions that may have about treatment.

Another short-term goal is writing and communicating current and reliable information. With social media grabbing headlines (Bowman and Willis 2003), it's imperative that reliable and accurate information be provided to employees, visitors, clients, and the media. The communications department/media information department can be a significant partner if utilized properly. It is imperative to ensure accurate and timely messaging is being delivered. If the company has a communications department, it must lead the process. If a company does not have a communications department, external consultants ought to be used. The communication plan needs to ensure that one strong, accurate message will be sent in a timely manner notifying all stakeholders regarding the status before, during, and after the crisis. It is also necessary to appoint one spokesperson for your organization. This individual should be part of the communications team and will be designated point person to answer all questions and inquiries.

The second challenge for the human resources department is establishing long-term goals. According to DHS (2017), "The long-term recovery process begins once the assembly areas are cleared by law enforcement for cleaning and the affected individuals have returned to their families and friends. The goals of long-term recovery are to help employees return to normality in their daily interactions and professional life, and to take whatever steps are necessary to return the facility and/or business to normal operations" (p. 6).

This is easier said than done. The physical or mental health status of many of the employees or their family members may never return to normal. It is imperative for human resources to continue

assisting and trying to resolve personal and work-related issues long after an incident (Wallace and Webber 2018).

Many smaller companies may not have a human resources department, security department, or emergency management department. What should they do after a crisis? They can implement strategies such as Hartford Distributors did after an active shooter event in August of 2010, in Manchester, Connecticut. An employee, Omar Sheriff Thornton, was given the option of resigning or being terminated by the company for allegedly stealing beer from the distributorship. After signing his resignation letter and being escorted from an office, Thornton removed two SR9 semiautomatic guns and began firing. He shot and killed eight coworkers and wounded two others. He then shot and killed himself. The company did not have an EAP, nor did they have trained counselors. However, Hartford Distributors reached out to surrounding companies in the community for guidance and assistance. The Manchester police department contacted area businesses in an effort to provide trauma counselors and ministers onsite, to assist with the grieving process.

Remember no two active shooter incidents are alike and no two businesses are alike. Architectural design, population, location, and employee makeup are not the same. Each business must prepare a plan for an active shooting event. Security professionals must survey their facilities and created a master plan dealing exclusively with their facility. In instance where you are a tenant of a multi-tenant building, you will need to interface with the building manager or property manager to ensure your plans interface effectively.

Stowell (2017) explained:

> Organizations affected by an active shooter event will face extraordinary challenges from the moment the first shot is fired. Even if the company is able to maintain business operations in the aftermath, the physical and emotional recovery can go on for months and years after the event. Besides reevaluating physical security measures, updating business continuity plans, and dealing with possible lawsuits, companies also have a responsibility toward their employees who have suffered severe emotional trauma. (p. 39)

Companies must weigh the options of when they can reopen their business and when it is a good time to do so. Stowell (2017) discussed the aftermath of the Hartford Distributors shooting by stating:

> An offsite location was being set up for business operations, but employees protested, saying they felt strongly about returning to the original facility as soon as possible. In the days following the shooting, 100 employees from other beer distribution plants in Connecticut, as well as in Rhode Island, came to assist the company in keeping business operations on track. A memorial service was held for the employees who lost their lives. The company president addressed workers on the front lawn, in front of a makeshift memorial, before they reopened their doors. (p. 42)

Sometimes locations where active shootings occurred are demolished to aid in the healing process. This was the case at the Sandy Hook Elementary School, in Newtown, Connecticut (Lysiak 2013). On December 14, 2012, 20-year-old Adam Lanza fatally shot 20 children between 6 and 7 years old, as well as six adult staff members. Prior to driving to the school, he shot and killed his mother in their Newtown home. Lanza committed suicide by shooting himself in the head.

After the horrific crime, the school was closed indefinitely. In January 2013 students returned to Chalk Hill Middle School in Monroe, Connecticut. Sandy Hook Elementary School was eventually demolished, and a new school was built not far from its original site. In July 2016 the new Sandy Hook Elementary school was opened.

Business Continuity

How does a business continuity plan impact business and the community after an active shooting? When a facility or a business closes due to a power outage, weather conditions, or any other reason, it is expected to reopen soon. Businesses create and implement detailed business continuity and

disaster management plans for their businesses so they can reopen quickly after an incident. Emergency managers often use the term recovery time objective (RTO). Snedaker (2007) writes "RTO is the time available to recover disrupted systems and resources. This is the time you have to get the systems back up and running" (p. 219). It is different when the business has to close for an active shooter incident. The memories, in particular if a coworker has died as a result of the shooting, never fade.

If the building is deemed a crime scene and cannot reopen for a few days, there are five areas your organization needs to address. First, consider issues experienced by your employees. Your company must ensure the employees feel safe and secure and the company's EAP is handling all issues, concerns, and questions that arise. That may require you to institute an employee 24-h hotline for assistance and perhaps increasing physical security (Wallace and Webber 2018).

Customer issues are the second concern. The business must ensure customers feel safe and secure and, despite the disruption in service, plans are in place to accommodate their needs.

The third issue involves facility-related concerns. What impact did the shooting have on the facility? Do rooms or offices have to be repainted? If laptops or important documents have been left behind, is there a process in place to retrieve them? Is your company familiar with the Corporate Emergency Access System (CEAS)? The CEAS program allows private-sector companies to apply for access cards for select employees, through a partnership with government, identifying them as "essential personnel" during a critical event, providing the ability to travel, enter affected areas, and service critical infrastructure (Wallace and Webber 2018). The CEAS program is located in the following locations: Baltimore, MD; Buffalo, NY; Philadelphia, PA; Stamford, CT; Erie County, NY; Commonwealth of Massachusetts; Nassau County, NY; New York City, all five boroughs; Rockland County, NY; State of Rhode Island; and Suffolk County, NY.

The fourth concern involves telecommunication issues. The business must consider whether there are enough available desks at other locations to accommodate employees who will be displaced. When phone systems have been impacted, the business will also need to consider what alternative plans can be made regarding the system. For example, can the network allow a specific number of employees to work remotely?

The fifth issue involves interfacing with external agencies. After an active shooter incident, it is imperative to advise employees and clients that the company has met or will be meeting with law enforcement agencies. Set up a town hall meeting with employees and family members of employees along with law enforcement agencies. Let the law enforcement agencies take the lead to discuss what happened, what they are doing, and what the company can do to try to prevent an incident like this from occurring again.

Conclusion

According to Stowell (2017), "In the case of an active shooter, U.S. companies are liable for protecting their employees as in any workplace violence incident. Under the U.S. Occupational Safety and Health Act of 1970, every U.S. employer is required to 'furnish to each of his employees' employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees' (p. 42). U.S. state and local provinces may also have their own relevant laws." There is protection for employees in the form of laws; however there is no guarantee that employees will feel safe in remaining in a workplace that has experienced an active shooting. The success and failure of a company will be based on their handling of an active shooter incident. How a company deals with an active shooter event before (planning and training), during (run–hide–fight), and after (recovery time objectives and robust EAPs) is

essential to the continuance of a company (Wallace and Webber 2018).

Cross-References

- ▶ Business Continuity Plan
- ▶ Educational Institution Safety and Security
- ▶ Physical Security: Best Practices
- ▶ Protection and Security in Public Spaces
- ▶ Workplace Violence: Assault
- ▶ Workplace Violence: Factors Contributing and/or Facilitating

References

APA (2019). Managing your distress in the aftermath of a mass shooting. Accessed at: https://www.apa.org/helpcenter/mass-shooting

Bowman, S., & Willis, C. (2003). We media: How audiences are shaping the future of news information. Reston, Va: The Media Center at the American Press Institute.

Burke, R. (2000). *Counter terrorism for emergency responders*. Boca Raton: CRC/Lewis Publishers.

Department of Homeland Security (2008). Active shooter – How to respond – Homeland Security. Accessed at: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf

Department of Homeland Security. (2017). Active shooter recovery guide. Accessed at: https://www.dhs.gov/publication/active-shooter-recovery-guide.

Lysiak, M. (2013). *Newtown: An American tragedy*. Gallery Books, A division of Simon & Schuster, Inc, NY, USA.

Silver, J., Simons, A., & Craun, S. (2018). A study of the pre-attack behaviors of active shooters in the United States Between 2000 – 2013. Federal Bureau of Investigation, U.S. Department of Justice, Washington, D.C. 20535.

Snedaker, S. (2007). *Business continuity & disaster recovery for IT professionals*. Burlington: Syngress Publishing.

Stowell, H. G. (2017). Security management: After an active shooter.

Wallace, M., & Webber, L. (2018). *The disaster recovery handbook* (3rd ed.). New York: Amacom.

Further Reading

Doss, K. T., & Shepherd, C. D. (2015). Active shooter. Preparing for and responding to an active threat, Oxford: Elsevier/Butterworth-Heinemann.

Haddow, G., Bullock, J., & Coppola, D. (2017). *Introduction to emergency management* (6th ed.). Waltham, MA: Butterworth-Heinemann.

Roig-Debellis, K., & Fisher, R. G. (2018). Choosing hope: How I moved forward from life's darkest hour. NY: G.P. Putnam's Sons.

Criminals: Blue-Collar Crimes

Hua-Lun Huang
Department of Sociology, Anthropology, and Child and Family Studies, University of Louisiana, Lafayette, LA, USA

Keywords

Survival-oriented crime · Expressive offense · Instrumental Offense · Social inequality

Definition

Blue-collar criminals tend to be from low income homes and their crimes involve physical or violent interactions. Since this population is constantly facing inadequate economic resources to satisfy their needs, they perpetrate blue-collar crimes in the context of economic pressure, financial need, or impoverishment.

Introduction

In criminology and criminal justice study, scholars usually agree that crimes can be committed by people of different social classes. Blue-collar crimes are survival-oriented (i.e., the main purpose/motivation for people to commit these crimes is to solve the problems of economic hardship, livelihood crisis, or extreme poverty). Since these offenses are largely committed by low-income or lower-class individuals (i.e., persons who frequently face the challenges of financial difficulty, economic scarcity, or shortage of income), such misbehaviors are called blue-collar crimes (or crimes of accommodation).

When criminologists/sociologists are inspecting the relationship between demographic factors and blue-collar crimes, the factors and the crimes chosen for inspection always have to be specific and definite. Blue-collar crimes can be classified into three broad categories in criminology and sociology: *property crime* (e.g., arson, burglary, and shoplifting), *violent crime* (e.g., bank robbery,

home invasion, and sexual assault), and *organized crime* (e.g., gang crime, human smuggling/trafficking, and illegal drug trading).

These categories, however, must be further classified so that criminologists and sociologists can perform research on blue-collar crime. Otherwise, the explanation or finding proposed by criminologists/sociologists may be invalid or unreliable because of design/ecological fallacy or other methodological problems (such as statistical error). In the next sections, the approach used by the Federal Bureau of Investigation in classifying property and violent crimes will be summarized. Then different typologies of arson, sexual assault, and homicide will be specified. This review will serve as a basis for categorizing blue-collar crimes in this article.

Legal (or Official) Classification of Crimes: Uniform Crime Report

In terms of classifying crimes, the most important (as well as popular) nomenclature used by criminologists and law enforcement authorities undoubtedly is the Uniform Crime Report (UCR). It was developed by the Federal Bureau of Investigation in the 1920s and 30s. According to this taxonomy, crimes can be classified into two principal categories – one is *serious offense* (i.e., Index crime), the other is *petty crime*.

Index crime includes two subcategories – one is *violent (or interpersonal) crime*, the other is *property offense*. Violent crime comprises four felonies: aggravated assault, forcible rape, robbery, and homicide. Likewise, property offense is composed of four felonies: arson, burglary, larceny, and motor vehicle theft.

Unlike Index crime which, almost without exceptions, involves heavy penalties like long prison sentences, offenses classified as petty crime (e.g., domestic abuse, shoplifting, simple assault, vandalism, violation of curfew, and so forth) usually can be settled through community services, fines, and/or other mild punishments. Partly because of this phenomenon, societal reaction to petty offenses usually is weak (or slow).

In a nutshell, the UCR was formulated by the FBI in the early twentieth century. As a result, it can be viewed as a standardized categorization system of crimes (see Fig. 1).

The Elaboration of Three Index Crimes: Arson, Rape, and Homicide

After the UCR has formally become a crime classification system in the 1970s, three Index offenses (i.e., arson, rape, and homicide) were elaborated by Douglas (who was a former FBI agent) and his colleagues in the early 1990s (see Douglas et al. 1997).

According to Douglas and his coworkers, arson can be instrumental (i.e., benefit-motivated) or expressive (i.e., emotion-driven). Instrumental arson includes, but is not limited to, six varieties: employment-related arson, survival-related arson, competition-related arson, insurance-related arson, inheritance-related arson, and crime concealment-related arson (especially, burglary-, larceny-, and murder-related arson).

Compared to instrumental arson (which may allow perpetrators to obtain enormous economic benefits, such as compensations offered by insurance companies), expressive arson provides offenders with an expedient outlet to relieve

Crimes

→ I. Index Crime
- → 1. Violent Crime → Aggravated Assault, Robbery, Rape, Homicide
- → 2. Property Crime → Arson, Burglary, Larceny, Motor Vehicle Theft

→ II. Petty Crime → Domestic Abuse, Driving under Influence, Shoplifting, Simple Assault, Vandalism, Violation of Curfew, and so forth

Criminals: Blue-Collar Crimes, Fig. 1 Offenses Categorized by the Uniform Crime Report

intense, uneasy, or troubled feelings (e.g., excitement, fury, hatred, jealousy, melancholy, and so on). It can be vandalism-related arson, attention seeking-motivated arson, hero arson, revenge-caused arson, extremist ideology-motivated arson, sexual arson, and serial arson.

Like arson, Douglas and his colleagues (1997) also divide sexual assault into two main categories. The instrumental one refers to those rape cases that take place in the context of sex slavery or searching for economic profits. For example, in criminal enterprise rape, sex traffickers can continually acquire pecuniary rewards if the victims they control persistently sell sex to customers (this trade is, of course, involuntary for the victim for they will be sexually assaulted by strangers again and again).

Besides criminal enterprise rape, both primary and secondary felony rapes are instrumental as well – the former refers to the situation that when someone (particularly young male) is perpetrating an Index crime like burglary, motor vehicle theft, or robbery, he accidentally finds an opportunity to commit sex crime. Like primary felony rape, secondary felony rape is also caused by profit-seeking behaviors. Nevertheless, this type of rape is premeditated for before perpetrating burglary, motor vehicle theft, or robbery, perpetrator has already had the intention to sexually assault any females he might encounter at the crime scene.

No matter whether primary felony rape is more common than secondary felony rape, expressive rape is, without doubt, far more diversified than instrumental one in pattern. This diversification can be clearly seen from the fact that at least 12 types of expressive rape are reviewed in *Crime Classification Manual* (CCM). They are social acquaintance rape (i.e., sexual assault perpetrated by acquaintances, which is most common among all types of rape), abduction rape, anger (or revenge-motivated) rape, domestic sexual assault, extremist ideology-motivated rape, group cause rape, power assertive rape, power reassurance rape, prison rape, religion- (or cult-) related rape, sadistic rape, and subordinate rape.

After classifying arson and rape from the angle of instrumental/economic or expressive/emotional motivation, Douglas and his associates (1997) do the same in CCM for homicide. According to this categorization, homicide can be instrumental manslaughter (i.e., murdering someone for money) or expressive killing (i.e., slaying someone because of emotional reasons). Instrumental homicide can be exemplified by seven types of homicidal behavior: contract killing, gang-related homicide, murder caused by criminal competition, insurance-related murder, inheritance-related murder, indiscriminate felony murder, and situational felony murder. In the commission of felony murder, the perpetrator has the intention to kill the victim or witness when committing an Index crime like burglary, motor vehicle theft, rape, or robbery. In the commission of situational felony murder, the perpetrator does not have the intention to kill the victim or witness when committing an Index crime; nevertheless, the victim or witness is still murdered because of a condition unanticipated by perpetrator.

Unlike instrumental homicide which is purely caused by the desire to obtain economic or financial benefits, expressive murder is far more complicated in motivation (i.e., it involves many noneconomic reasons or purposes like anxiety, anger, control, domination, fantasy, gender/racial bias, and so on). With this in mind, explaining this type of homicidal behavior is always a sophisticated process for criminologists and crime investigators.

In any event, expressive homicide basically originates from highly distressed, disturbed, or distraught feelings/emotions. According to the classification of CCM, it can be argument-triggered murder, authority killing, domestic homicide, group cause homicide, hero homicide, mercy homicide, revenge-related homicide, and sexual homicide. The various types of arson, rape, and homicide discussed above suggest that blue-collar crime is an extremely intricate concept for not only can it be divided into interpersonal and property offenses, it can be classified into instrumental and expressive misconducts as well.

Categories of Blue-Collar Crime: Some Examples

Based on the discussion above, it seems adequate to argue that both crime concealment-related arson

(especially, burglary-, larceny-, and murder-related arson) and vandalism-related arson are some textbook examples of blue-collar crime. The reason for this is that according to studies and statistics (see Clinard et al. 1994; Frailing and Harper 2016; Holmes and Holmes 2009), both crime concealment-related arson (CCRA) and vandalism-related fire-setting (VRFS) are chiefly committed by people of blue-collar/low-income families in the context of economic dilemma, financial struggle, and/or hostility toward society.

Besides CCRA and VRFS, the following types of rape appear to be good examples of blue-collar crime as well:

- Criminal enterprise rape (i.e., sexual assault involved by prostitution rings)
- Primary felony rape (i.e., sexual assault committed by burglars, home intruders, or motor vehicle thieves as a result of chance)
- Secondary felony rape (i.e., sexual assault committed by burglars, home intruders, or motor vehicle thieves because of premeditation)
- Abduction rape (i.e., sexual assault perpetrated by abductors)
- Group cause rape (especially sexual assault perpetrated by gang members)
- Prison rape (i.e., sexual assault perpetrated by inmates, most of whom tend to come from working-class or lower-class families)

Finally, certain categories of homicide can also serve as model examples of blue-collar crime for in America, they were chiefly committed by low-income young males (see Holmes and Holmes 1994; Katz 1988). These homicidal behaviors include

- Gang-related homicide (i.e., manslaughter committed by hostile street gangs for the purpose of controlling turf or an illegal business)
- Indiscriminate felony murder (i.e., perpetrator has the intention to kill the victim or witness when committing an Index crime like burglary, motor vehicle theft, rape, or robbery)
- Situational felony murder (i.e., perpetrator does not have the intention to kill the victim or witness when committing an Index crime; nevertheless, the victim or witness is still murdered because of a condition unanticipated by perpetrator)
- Argument-triggered murder (i.e., homicide perpetrated by young people, particularly young males, who are at odds in a bar, tavern, public billiard room, strip club, or other places where conflicts between strangers can take place easily)
- Domestic homicide (i.e., murder perpetrated by family members, especially members of low-income Black families)

All of the categories of arson, sexual assault, and homicide listed above indicate that blue- collar crime is a tremendously complicated theme in criminology for it involves many offenses that differ in choice structuring properties – some are violent and highly risky (e.g., bank robbery), some are nonviolent and "fairly safe" (e.g., credit card fraud), some require special skills and trainings (like professional burglary), while some are nonviolent, "fairly safe," and do not entail expertise (e.g., shoplifting). Because of this complicity (see Table 1), it is obvious that researchers must clearly define their subject matter when addressing the issue of blue-collar crime.

Blue-Collar Workers/Criminals

Blue-collar crimes tend to be easier for the public to observe and experience, as well as for the authorities to investigate. Such phenomenon seems to be strongly related to the fact that most blue-collar workers do not possess an independent working space (e.g., personal office) or enjoy autonomy when performing a job. In other words, the actions of blue-collar workers during working hours normally are overseen by colleagues or supervisors and thus are observable. For this very reason, blue-collar crimes usually are perpetrated in open or public places (e.g., downtown districts of a big city, parking lots, railway stations, shopping malls, slum areas, tourist hotspots, and so forth), instead of in indoor or private settings where deviant or criminal behaviors can be easily committed in secret.

Criminals: Blue-Collar Crimes, Table 1 Some Representative categories of blue-collar crime

	Property crime	Violent crime	Organized crime
Instrumental offense [Main function: helping blue collar workers/low-income people cope with economic stress or financial dilemma]	Arson: • Burglary-related arson • Larceny-related arson • Murder-related arson	Rape: • Criminal enterprise rape • Primary felony rape • Secondary felony rape • Abduction rape Homicide: • Gang-related murder • Indiscriminate felony murder • Situational felony murder	• Nonprofessional burglary • Professional burglary • Human trafficking • Drug trading
Expressive offense [Main function: serving as an outlet for blue color workers/low-income people's resentment or other negative emotions]	• Vandalism-related arson	Rape: • Group cause rape • Prison rape Homicide: • Argument-triggered murder • Domestic homicide	• Hate crime (perpetrated by those blue collar workers/ lower-class people who firmly believe they are exploited by cold-blooded economic elites) • Criminal cult crime

The research clearly indicates that there is a positive relationship between blue-collar workers/low-income persons and blue-collar crimes.

From the viewpoint of conflict theory or Marxism, all human societies on earth (no matter whether they are ancient or contemporary) are unequal in the distribution of economic resources (even those high-income countries that have sound social security system, like Denmark, Finland, Norway, and Sweden, are not purely equal). Because of this global problem, most governments in the modern world must deal with the problem of poverty and unemployment on a regular basis.

Unfortunately, no government, at least so far, can completely solve the problems of poverty and unemployment (probably because of insufficient economic resources or inadequate economic policy). Accordingly, some individuals (especially the truly advantaged and the underclass; see Wilson 1990) fall into in deep or permanent poverty – for these persons, improving socioeconomic status is extremely difficult, if not impossible, because they do not possess those assets (e.g., college education and professional degree) that will allow people to get a prestigious or high-paying job. Unable to obtain a professional or higher-paid job, of course, suggests that low-income people (including some blue-collar workers) will keep facing the problem of poverty.

Given that certain blue-collar workers and lower-class people are the least resourceful persons in a society, these populations naturally do not have many options in handling the economic pressure caused by financial difficulty. In this regard, perpetrating crimes seems to be an effective approach in helping less resourceful individuals acquire

economic/financial resources because this tactic (even though it is illegal) does not require academic degree or investments.

In any event, blue-collar crimes tend to have the following four characteristics in common:

First, they do not originate from power, property, or prestige; instead, they spring from shortage of economic resources or economic predicament caused by unemployment (Geis and Meier 1977; Simon 2018). Second, such crimes (like burglary, drug trade, and robbery) can help some blue-collar workers and lower-income people solve short-term economic crisis (Shover and Wright 2000). Third, such crimes (e.g., burglary, shoplifting, and robbery) normally are perpetrated in places where the public can act as witnesses or interventionists. Finally, such crimes (e.g., arson, rape, and robbery) usually are not subtle or silent.

Although less typical, blue-collar or low-income individuals may also commit "white collar crimes" (i.e., crimes stemmed from power, property, or prestige). For example, blue-collar workers who serve as cashiers in a workplace that requires manual labor (e.g., auto body shop, manufacturing plant, and restaurant) will gain opportunities to access cash or other financial resources. The authority of handling cash or other assets then gives working-class or lower-class individuals opportunities to commit financial crimes, like embezzlement or larceny.

Conclusion

In this entry, the defining characteristics of blue-collar crimes, three representative categories of blue-collar crimes (i.e., arson, rape, and homicide), and some demographic features of blue-collar criminals are inspected. This inspection shows that blue-collar crimes mainly originate from social inequalities (particularly income, racial, and gender inequalities). Instrumental offenses (like burglary, shoplifting, and robbery) therefore can help some blue-collar persons/low-income people cope with (short-term) financial crisis.

In addition to instrumental offences, blue-collar crimes can be expressive offenses as well (e.g., domestic abuse, family violence, rape, and manslaughter). These "emotional crimes" usually are committed by those blue-collar workers/lower-class people who have heavy psychological burden (because of financial strain) or are annoyed by social environments. As a result, blue-collar crimes can be considered as desperate means used by certain working- or lower-class people to adapt to economic strains (or to alleviate emotional tensions).

Cross-References

- ▶ Criminals: Motives
- ▶ Criminals: White-Collar Crimes
- ▶ Investigations: Criminal

References

Clinard, M. B., Quinney, R., & Wildeman, J. (1994). *Criminal behavior systems: A typology* (3rd ed.). Cincinnati: Anderson Publishing Company.

Douglas, J. E., Burgess, A. W., Burgess, A. G., & Ressler, R. K. (1997). *Crime classification manual: A standard system for investigating and classifying violent crimes*. San Francisco: Jossey-Bass Publishers.

Frailing, K., & Harper, D. W. (2016). *Fundamentals of criminology: New dimension*. Durham: Carolina Academic Press.

Geis, G., & Meier, R. F. (Ed.). (1977). *White-collar crime: Offenses in Business, Politics, and the Professionals*, revised edition. New York: The Free Press.

Holmes, R. M., & Holmes, S. T. (1994). *Murder in America*. Thousand Oaks: Sage.

Holmes, R. M., & Holmes, S. T. (2009). *Profiling violent crimes: An investigative tool* (4th ed.). Thousand Oaks: Sage.

Katz, J. (1988). *Seductions of crime: Moral and sensual attractions in doing evil*. New York: Basic Books.

Shover, N., & Wright, J. P. (Eds.). (2000). *Crimes of privilege: Readings in white-collar crime*. New York: Oxford University Press.

Simon, D. R. (2018). *Elite deviance* (11th ed.). New York: Routledge.

Wilson, W. J. (1990). *The truly advantaged: The inner city, the underclass, and public policy*. Chicago: University of Chicago Press.

Further Reading

Canter, D., & Alison, L. (Eds.). (2000). *Profiling property crimes*. Burlington: Ashgate.

Katz, M. B. (Ed.). (1993). *The "underclass" debate: Views from history*. Princeton: Princeton University Press.

Quinney, R. (2001). *The social reality of crime*. New Brunswick: Transaction Publishers.

Criminals: Cybercriminals

George Grispos
School of Interdisciplinary Informatics,
University of Nebraska Omaha,
Omaha, NE, USA

Keywords
Cybercriminal · Digital crime · Digital criminal

Definition

Cybercriminals commit or support criminal acts in a digital world. These acts can be classified as either *digital-focused* crimes, where a criminal act has emerged as result of technology, or *digital-assisted* crimes, where a criminal has used technology in a supporting capacity to commit a criminal act.

Introduction

Industry reports indicate that cybercriminals continue to target organizations around the world. The PricewaterhouseCoopers (PWC 2018) Global Economic Crime and Fraud Survey indicated that a third of all respondents had been a target for cybercriminals. The survey also reported that a quarter of the respondents were victims of digital extortion or had suffered from asset misappropriation during the last year. These increases come at a great financial cost. The 2017 Ponemon Cost of Cybercrime report estimated that the financial losses from criminal enterprise cost organizations an average of $11.7 million in 2017, an increase of 23% since the previous year and a 62% increase over the last 5 years (Ponemon Institute 2017).

The reality is that the continuous amalgamation of technology into everyday life is creating an environment that is potentially conducive to cybercrime (Grispos 2016; Grispos et al. 2019). Cisco (2011) summarized the problem with the quote "wherever users go, cybercriminals will follow" (p. 14). Hence, there is a need to discuss the impact of cybercrime on society, examine who is involved in cybercriminal activities, and investigate how cybercriminal behaviors can be effectively reduced. This entry examines the historical perspective of cybercrime, defines and characterizes cybercriminals through various demographics, and discusses what, potentially, motivates cybercriminals. The entry concludes by presenting an overview of various strategies that are being undertaken to counter cybercrime.

History of Cybercriminals

One of the first documented cases of cybercriminal activity took place in November 1988, when a university student called Robert Morris wrote a computer worm (aka the "Morris Worm"). This computer worm infected the Advanced Research Projects Agency network (ARPAnet) and resulted in 10% of the computer systems attached to ARPAnet to be shutdown. The Morris Worm also infected systems within many universities, medical research facilities, and military buildings. Morris was eventually convicted of violating United States Code Title 18, the Computer Fraud and Abuse Act and was sentenced to 3 years of probation, 400 hours of community service, and fine of $10,050 (Markoff 1990). However, one positive outcome from the Morris Worm was the establishment of the Computer Emergency Response Team Coordination Center (CERT/CC), whose purpose is to provide a central point for coordinating responses to "Internet" attacks by cybercriminals.

Since the 1980s, the number of individuals and organizations that rely on computers for their business records and other functions, both in closed (i.e., only connected within the company) and open (i.e., connected to computers within and outside the company) networks, has grown exponentially. Hence, there is a growing demand for individuals and organizations to secure personal and customer information, as well as systems that are used to process and store this information. However, the software and applications that are

executed on these systems are often vulnerable to a variety of cyberattacks, forcing software manufacturers to either release updates to prevent attacks or worse, repair the damage caused by cybercriminals. For example, malware authors around the world have caused millions of dollars in damages through computer viruses and computer network worms such as Melissa, Love Bug, and Code Red (Hoar 2005). Likewise in 2003, the SQL Slammer worm resulted in millions of individuals around the world to go without cellular or Internet service as well as the cancellation of flights from airports in the United States (Hoar 2005).

The past few years has also seen a rise in a new type of cybercrime, committed not just by individuals, but by state-sponsored groups. For example, a North Korean-backed hacking group was considered to be responsible for an attack on the film production company, Sony Pictures. This attack resulted in personal information and intellectual property being obtained and released to the general public. However, what is more concerning is that many of these state-sponsored groups now aim to cause physical damage through the digital world (Grispos et al. 2017). As a result, these cybercrimes have resulted in physical damage to buildings, the shutdown of nuclear reactors, and even medical hospitals closing their doors to patients (Loukas 2015).

Defining Characteristics of Cybercriminals

An analysis of the literature suggests that a general consensus on the term "cybercriminal" has yet to emerge, and this is perceptible in the following descriptions:

- "person (who) uses the Internet, computers and related technology in the commission of a crime" (Maras 2016, p. 4)
- "is a person who commits an illegal act using a computer with an ulterior (m)otive" (Chouhan 2014, p. 49)
- "individuals (who exploit) the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that knows no borders, either physical or virtual" (INTERPOL 2018, p. 1)

While there is much ambiguity surrounding the definition of a cybercriminal, there have also been attempts to characterize cybercriminals from the perspective of their gender, ethnicity, and social interactions with other criminals. Several researchers have argued that most cybercriminals are *male* (Bachmann 2010; Cueto 2015; Jordan and Taylor 1998; Motoyama et al. 2011). One potential reason is that there are more male than female computer science majors enrolled in universities who subsequently become programmers, who can, potentially, turn into hackers (Cueto 2015). Evidence for this theory is visible in the number of male cybercriminals who have been arrested and prosecuted for a variety of cybercrimes. For example, Kevin Mitnick obtained unauthorized access to systems belonging to Digital Equipment Corporation, Pacific Bell, and several United States Government agencies. Mitnick was eventually prosecuted and served 5 years in prison. Similarly, Michael Calce was sentenced to 8 months "open custody" for launching several Denial-of-Service (DoS) attacks against organizations including Yahoo, eBay, and CNN.

An alternative demographic that has been examined in more detail in the last decade is related to the *race/ethnicity* of cybercriminals. The evidence suggests that most cybercriminals are Asian or of European descent, given that these are the racial backgrounds of most programmers (Cueto 2015). Moreover, this notion has been fueled by a growing number of cybercriminal incidents that are purported to have originated in countries, such as North Korea, China, and Russia. For example, Kozlowski (2014) examined three cyberattacks on Estonia in 2007, Georgia in 2008, and Kyrygysytan in 2009, with the aim of answering who was responsible and why the attacks were undertaken. Kozlowski (2014) concluded that in all three cases, these countries had tense relations with Russia, and that attacks were either carried out by patriotic cybercriminals on behalf of the Russian government or by

the Russian government itself. Russian cybercriminals continue to be attributed for a variety of cybercrimes, including a number of attacks that resulted in American companies losing tens of millions of dollars due to scams and fraudulent activities (Gregorian 2018). Similarly, as China's internet presence continues to increase, the state of cybercrime in China has been the focal point for several studies (Kshetri 2013; Lewis 2005; Yip 2011). Kshetri (2013) has reported that China often ranks in the top three countries for hosting malware, generating spam, click fraud, and being responsible for cyberattacks.

While most cybercriminals are understood to act alone, many cybercrimes are not committed in isolation (Hutchings and Chua 2016). For example, cybercriminals will compromise servers to steal credit card information, then compromise another server to store and sell this information in the near future (Hutchings and Chua 2016). This can complicate efforts to identify and associate crimes with a particular cybercriminal or group. Further confusing matter is the emergence of organized cybercriminal groups (Choo and Smith 2008). While individuals within these groups are considered highly technical cybercriminals, they are unlikely to know each other in the physical world (Choo and Smith 2008). Therefore, unless digital evidence can be found exposing a cybercriminal's organizational topology, some group members might never be known to law enforcement investigators.

Cybercriminal Motivations and Activities

Cybercriminals can be motivated by a variety of reasons to commit criminal acts, including social, political, religious, economical, revenge, and thrill-seeking motives. In the leaked classified American intelligence case, Chelsea (Bradley) Manning claimed that the information was disclosed to raise awareness of the wars in Afghanistan and Iraq, effectively *cyber-activism* (Thorsen et al. 2013). Likewise, Kevin Mitnick has often stated that committing his cybercrimes was more for fun and to challenge himself intellectually (Shimomura and Markoff 1995). However, on the other side of the spectrum are cybercriminals who commit crimes as part of a political statement or as part of an organized crime syndicate. An example of a political cybercrime is the 2014 Sony hacking by North Korea, who objected to the screening of "The Interview" and threatened to attack American cinema theaters who screened the film (Haggard and Lindsay 2015). Similarly, cybercriminals such as Nicolae Popescu who was part of a much larger group of individuals that were responsible for a wide variety of fraudulent financial activities (Lusthaus and Varese 2017).

In order to fulfill these motivations, cybercriminals will undertake a variety of different activities. Wall (2007) argued that there are three generations of cybercriminal activities: *crimes in the machine* (i.e., computer content), *crimes using machines* (i.e., computer related), and *crimes against the machine* (i.e., computer integrity). Wall (2007) speculated that in the future, cybercriminal and victim interaction will be completely automated by technology and therefore, removing the need for victim interaction. In addition to Wall's classification, several organizations and governmental bodies have attempted to develop taxonomies that define and determine a range of cybercriminal activities. However, a consensus on what should be included in these taxonomies has yet to materialize. For example, the United Kingdom's National Crime Agency's (2018, p. 1) taxonomy of cybercriminal activities include:

- Phishing – email messages asking for either security information or personal details
- Hijacking – when a cybercriminal controls your webcam, or hijacks files on a digital device and holds them ransom, usually until a financial payment is made
- Keylogging – where a cybercriminal records what is typed on a computer's keyboard or obtains screenshots of the victim's computer screen
- Ad clicking – cybercriminals directing a victim's computer, after the victim has clicked a specific link, which is often malicious
- Hacking – cybercriminals who gain unauthorized access to a computer system

- Distributed Denial of Service (DDoS) attacks – cybercriminals who attempt to disrupt the availability and "connect-ability" of a computer system

The Australian Cybercrime Online Reporting Network (2018, p. 1) provides an alternative taxonomy describing cybercriminal activities, which in some cases focus on traditional crimes where cybercriminals have extended their effect into the digital world:

- Attacks on computer systems – this includes hacking, malware, and viruses.
- Cyber-bullying – online behavior that is intended to make victims fearful and could also result in harassment.
- Prohibited offensive and illegal content – viewing, distributing, or promoting digital content that has been considered illegal or prohibited in a specific jurisdiction.
- Online child sexual abuse material – viewing, distributing, or promoting material that shows child sexual abuse. This includes grooming and sexting.
- Identity theft – cybercriminals misusing personal information or online accounts that belong to the victim.
- Online trading issues/Online scams or fraud – illegal activities related to buying or selling online.
- Email spam and phishing – cybercriminals distributing unwanted email messages or promoting material to obtain personal information from a victim.

The aforementioned techniques used by cybercriminals lead to a variety of consequences that range from minor to severe. For example, the WannaCry hack that resulted in messages from hackers demanding ransom payments resulted in 327 payments totaling $130,000 (Gibbs 2017). However, the WannaCry hack also impacted several National Health Service (NHS) hospitals in the United Kingdom, which cumulated in 19,000 medical appointments to be cancelled (Field 2018). Similarly, in 2018 Under Armour revealed that its MyFitnessPal mobile app had been hacked, which resulted in 150 million accounts being compromised. Usernames, email addresses, and hashed passwords were stolen (Lamkin 2018). Many of these user details were placed for sale on the dark web on websites such as Silk Road, an online black market (Hong 2015). Once these details are purchased by other cybercriminals, they can be used to commit additional cybercrimes (i.e., identity theft). For example, Amar Singh and his spouse Neha Punjani-Singh were found guilty of identity theft and credit card scams that resulted in victims losing $13 million (Carrega-Woodby 2012).

Countering Cybercriminals

The increasing rate of cybercrime prompts the discussion on the implementation of countermeasures to deter cybercriminals from committing such acts. These countermeasures can be broadly classified any *actions*, *technology*, or *devices* that can be applied with the purpose of preventing or mitigating the impact of a cybercrime (MacKinnon et al. 2013). It must be noted that no single solution exists to counter cybercrime, and that a number of legal and behavioral countermeasures are often needed to prevent cybercriminals from succeeding.

From a legal perspective, the increasing impact and costs associated with cybercrime has prompted European nations along with Canada, Japan, and the United States to ratify the Budapest Convention on Cybercrime (Council of Europe 2001). The purpose of this international treaty was to counter computer-related criminal activities through increased cooperation between national law enforcement agencies, harmonizing related laws, and improving the quality of cybercriminal investigations. Similarly, efforts had also been made to bring cybercriminals to justice in the International Criminal Court (Ophardt 2010).

Thus far, legal countermeasures have often been insufficient. Consequently, many organizations have implemented behavioral countermeasures in an effort to counter offenses by cybercriminals. These types of countermeasures range from raising public awareness to

educating the community on defining cybercrime, detecting and reporting cybercriminal activities, implementing policies and technical safeguards, as well as educating and training the population on safe cyber-practices (Yang and Hoffstadt 2006). Alternatively, many financial organizations such as banks, are choosing to implement biometric countermeasures (methods that rely on physical or behavioral traits, such as a fingerprint) in order to prevent cybercrimes from transpiring.

Conclusions

Cybercriminals are a distinct type of criminal, who engage in devious behavior involving some form of technology. While a consensus on the definition of the term "cybercriminals" or their activities has yet to emerge, it is very difficult for organizations and governments to ignore the problem. This is because the focus of cybercriminal activity has moved from attacks that temporarily disrupt research networks and steal classified intellectual property of the company and/or their clients' personal information to hijacking that literally shut down medical hospitals and delay patient treatments until the ransom is paid. Hence, ordinary citizens are now being impacted by cybercrime even though they are not the intended target. Therefore, it is imperative that organizations and businesses have the ability to identify, define, and investigate cybercrime, when it occurs. This means providing these organizations with tools, techniques, and laws to counter cybercriminals as they change face in the coming decades.

Cross-References

► Investigations: Cybercrimes

References

Australian Cybercrime Online Reporting Network. (2018). Learn about cybercrime. Retrieved from https://www.acorn.gov.au/learn-about-cybercrime

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*, 643–656.

Carrega-Woodby, C. (2012). Queens couple pleads guilty to roles in largest ID theft scam in US history. Retrieved from https://nypost.com/2012/08/06/queens-couple-pleads-guilty-to-roles-in-largest-id-theft-scam-in-us-history/

Choo, K.-K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology, 3*(1), 37–59.

Chouhan, R. (2014). Cyber crimes: Evolution, detection and future challenges. *IUP Journal of Information Technology, 10*(1).

Cisco. (2011). Cisco 2011 annual security report.

Council of Europe. (2001). Convention on cybercrime.

Cueto, J. (2015). Race and gender among computer science majors at Stanford. Retrieved from https://medium.com/@jcueto/race-and-gender-among-computer-science-majors-at-stanford-3824c4062e3a

Field, M. (2018). WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled. Retrieved from https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Gibbs, S. (2017). WannaCry: hackers withdraw £108,000 of bitcoin ransom. Retrieved from https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom

Gregorian, D. (2018). Feds say Russian hackers duped U.S. companies out of tens of millions in advertising dollars. Retrieved from https://www.nbcnews.com/news/us-news/feds-say-russian-cybercriminals-duped-u-s-companies-out-tens-n940946

Grispos, G. (2016). *On the enhancement of data quality in security incident response investigations*. University of Glasgow.

Grispos, G., García-Galán, J., Pasquale, L., & Nuseibeh, B. (2017). *Are you ready? Towards the engineering of forensic-ready systems*. Paper presented at the 11th international conference on research challenges in information science (RCIS), Brighton, United Kingdom.

Grispos, G., Glisson, W., & Cooper, P. (2019). *A bleeding digital heart: Identifying residual data generation from smartphone applications interacting with medical devices.* Paper presented at the proceedings of the 52nd Hawaii international conference on system sciences. Maui, HI, USA.

Haggard, S., & Lindsay, J. R. (2015). North Korea and the Sony hack: Exporting instability through cyberspace. *Asia-Pacific Issues* (117), 1.

Hoar, S. B. (2005). Trends in cybercrime: The dark side of the Internet. *Criminal Justice, 20*, 4.

Hong, N. (2015). Silk road creator found guilty of cybercrimes. Retrieved from https://www.wsj.com/articles/silk-road-creator-found-guilty-of-cybercrimes-1423083107

Hutchings, A., & Chua, Y. T. (2016). Gendering cybercrime. In *Cybercrime through an interdisciplinary lens* (pp. 181–202). Routledge. New York, NY, USA.

INTERPOL. (2018). Cybercrime. Retrieved from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757–780.
Kozlowski, A. (2014). Comparative analysis of cyber-attacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal, 10*(7), 237–245.
Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. *Electronic Commerce Research, 13*(1), 41–69.
Lamkin, P. (2018). Under Armour admits huge MyFitnessPal data hack. https://www.forbes.com/sites/paullamkin/2018/03/30/under-armour-admits-huge-myfitnesspal-data-hack/
Lewis, J. A. (2005). Computer espionage, Titan rain and China. *Center for Strategic and International Studies-Technology and Public Policy Program, 1*.
Loukas, G. (2015). *Cyber-physical attacks: A growing invisible threat*. Oxford: Butterworth-Heinemann.
Lusthaus, J., & Varese, F. (2017). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice, PAX042*, 1–11. https://doi.org/10.1093/police/pax042
MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). Cyber security countermeasures to combat cyber terrorism. In *Strategic intelligence management* (pp. 234–257). Elsevier. Waltham, MA, USA.
Maras, M.-H. (2016). *Cybercriminology.* Oxford University Press, Oxford, United Kingdom.
Markoff, J. (1990). Computer intruder is put on probation and fined $10,000. *The New York Times*.
Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). *An analysis of underground forums.* Paper presented at the proceedings of the 2011 ACM SIGCOMM conference on internet measurement conference. Berlin, Germany.
National Crime Agency. (2018). Cyber crime. Retrieved from http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime
Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duke Law & Technology Review*, i.
Ponemon Institute. (2017). 2017 cost of cyber crime study.
PWC. (2018). *Global economic crime and Fraud survey.* https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
Shimomura, T., & Markoff, J. (1995). *Takedown: The pursuit and capture of Kevin Mitnick, America's most wanted computer outlaws-by the man who did it*. New York: Hyperion Press.
Thorsen, E., Sreedharan, C., & Allan, S. (2013). Wikileaks and whistle-blowing: The framing of Bradley manning. In *Beyond WikiLeaks* (pp. 101–122). Springer. London, United Kingdom.
Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183–205.
Yang, D. W., & Hoffstadt, B. M. (2006). Countering the cyber-crime threat. *American Criminal Law Review, 43*, 201.
Yip, M. (2011) An investigation into Chinese cybercrime and the applicability of social network analysis. *ACM WebSci '11, Koblenz, Germany.*

Further Reading

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic. Waltham, MA, USA.
Rogers, M. K. (2011). The psyche of cybercriminals: A psycho-social perspective. In *Cybercrimes: A multidisciplinary analysis* (pp. 217–235). Springer. Berlin, Heidelberg.
Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters, 58*(1), 22–23.

Criminals: Motives

Jennifer Bencivenga
John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Motive · Crime · Gang · MS-13 · Revenge · Workplace violence · Greed · White collar crime · Drugs · Alcohol · Addiction · Love · Murder-suicide · Munchausen syndrome by proxy

Definition

Criminal motives are those causes that invoke illegal actions.

Introduction

Criminal motives are those causes that invoke illegal actions. For an action to be considered illegal, an applicable law must be broken. For an illegal action to be considered criminal, the offense must cause harm to society or property. Criminal motives shed light on the "why?" behind deviant behavior and, when coupled with evidence in court, provide jurors with additional support in considering verdict.

Often confused with intent, motive constructs are external antecedents to internal thought processes (Maasberg et al. 2015). In this sense, motive and intent are two different elements with the former influencing the latter. Common law is founded on the principle that an individual is guilty of a crime when there is both a guilty action (actus reus) and guilty mind (mens rea). In Latin, *Actus non facit reum nisi mens sit rea*, or "an act is not necessarily a guilty act unless the accused has the necessary state of mind required for that offense" (Gooch and Williams 2015). Understanding a motive's impact on intent is fundamental when determining criminal punishment, as is considering the seriousness of the crime committed.

There are several ways to classify crimes; however, based on the severity of punishment, crimes can be grouped into four separate categories: felonies, misdemeanors, felony-misdemeanors, and infractions. Criminal law defines crimes within these categories to include violent crimes, such as homicide, rape, robbery, aggravated assault, burglary, larceny theft, motor vehicle theft, and arson, as well as less serious crimes, such as simple assault, fraud, vandalism, drug abuse violations, gambling, and vagrancy, to name a few.

Though federal and state law explicitly categorizes crimes, the motives that drive individuals to commit crimes are not as easily discerned. For centuries, theorists have researched and analyzed the criminal motivations that drive individuals to commit crimes. It is theorized that biological, psychological, sociological, and biosocial factors may impact decisions to commit illegal actions. However, it is also understood that more distinguishable triggers primarily impact an individual or group to act in an aberrant way. By defining criminal motives, investigators are better equipped to bring alleged criminals to justice.

Gang Membership

In law enforcement, gang dynamics is a fiercely studied and analyzed topic. Gang culture may attract potential individuals for a multitude of reasons and encourage a lifestyle that often leads to criminal activity. From acceptance to ongoing affiliation, members are motivated by both internal and external factors. Motivations often include identity or recognition (achieve a level of status), protection, fellowship/brotherhood, intimidation, and criminal activity resulting in financial gain (LAPD n.d.).

Depending on the group and region of matriculation, gangs and their leadership may require potential associates and recognized members to commit illegal acts to pledge allegiance and ongoing alignment to the group. Several different types of gangs exist, including prison, street, and outlaw motorcycle, with some groups being much more violent than others. For example, Mara Salvatrucha or MS-13 gang crimes are not primarily petty nuisance crimes; since 2012, of 500 cases reviewed by the Center of Immigration Studies, 207 MS-13 members were charged with murder. Additionally, more than 100 were accused of conspiracy/racketeering and dozens of others for drug trafficking, sex trafficking, attempted murder, sexual assaults, and extortion (Vaughan 2018).

Revenge

Synonymous with retaliation and retribution, revenge is an act of justice. Born from passion, revenge motivates individuals to hurt or harm someone for a perceived injustice. Though it is often associated with love triangles, revenge manifests itself in other relationships and environments. One prevalent and increasingly violent form of revenge renders itself in workplace violence. Some 2 M American workers are victims of workplace violence each year, and of note, in 2014, 16% of all workplace deaths were attributed to work-related attacks (National Safety Council 2018). Criminal acts of revenge in the workplace may include harassing or indecent communications, physical assault, or murder.

Though revenge is generally associated with adult behavior, it also occurs naturally within youth. Findings from a recent study conducted on 5,373 youth indicate that approximately one-half of interpersonal assaults were motivated by revenge and that a significant proportion (10–20%) of running away from home and vandalism incidents were also related to revenge (Kivivuori et al. 2016).

Greed/Money

Greed refers to the desire to always want more, yearning to fulfill some type of unsatisfied state of mind. Individuals experience greed in several aspects of life, one example being with financial gain. In this sense, greed may manifest itself in an addictive state and result in habitual gambling or with petty crime, i.e., larcenies, thefts, burglary, or robbery.

In regard to business and politics, greed often leads to corruption. For example, Enron, WorldCom, Tyco, and Freddie Mac were all big businesses that suffered great scandal after executives and leadership were the subjects of white-collar crime accusations. Recent studies have found that other factors, in addition to greed, may also motivate white-collar criminals to commit fraudulent acts. One major concept is that of convenience; that "convenience is a relative concept where white-collar crime is chosen over legitimate actions when there is a strong economical motive, ample organizational opportunities, and acceptance of deviant behavior" (Gottschalk 2018).

Drugs and Alcohol

Though drugs and alcohol are not direct motivations associated with crime, their effects on the human mind may trigger certain responses that ultimately lead to criminal behavior. In fact, approximately 80% of offenses leading to incarceration in the United States involve alcohol or drugs (NCADD n.d.). Drug offenses may include possession, distribution, specialized distribution offenses, improperly obtaining drugs from those in legal possession, drug crimes against children, and conspiracy. Alcohol offenses may include minor in possession, unlawful transportation, public drinking, driving while intoxicated, and operating under the influence.

Individuals with an addiction to drugs or alcohol are more likely to be involved with rapacious crimes. In 2016, 11.5 M people misused prescription opioids, and 116 people died every day from opioid-related drug overdoses (USDHHS n.d.). To score a fix, users may result to larceny, shoplifting, breaking and entering, and robbery. In more serious cases, addicts may solicit themselves or commit homicide for drugs.

Love

Even love renders itself in crime. Incidents may derive from domestic disputes, non-intimate partner domestic violence, familial arguments, and disagreements with friends. Some of the most horrific incidents that are perceived as acts of love are murder-suicides. More than 1,300 people died in murder-suicides in America in 2017, and during a 6-month period, 42 homicide victims were less than 18 years of age (Violence Policy Center 2018). Murder-suicide triggers may include money troubles, recent separation or divorce, custody battles, and ongoing domestic violence.

Another crime committed out of perceived love is a type of medical child abuse when a caregiver imposes a fictitious illness on a victim. This act of medical child abuse is referred to as Munchausen syndrome by proxy. By imposing a disorder on a child, the caregiver, generally the mother, feels appreciated and needed. A recent study analyzed 796 perpetrators from case reports and case series and concluded that "mothers with a personal history of childhood maltreatment, obstetric complications, and/or factitious disorder are at heightened risk for medical child abuse" (Yates and Bass 2017). By evaluating the medical history of potential perpetrators, investigators can better understand probable motives.

Conclusion

Inherently, certain crimes are linked to certain motives. Though motives may be predictive of crimes, not every crime is a result of one single motive. In fact, various motives may lead to one particular crime. For example, a gang member may commit murder on a rival gang member on behalf of the affiliated gang and because of a personal need for revenge. Or a habitual drug user may be a suspect in a domestic violence incident resulting from a disagreement. For this reason, it is essential that security professionals and law enforcement understand criminal motives, as motives tell the crime story.

Cross-References

- ▶ Criminals: White-Collar Crimes
- ▶ Investigations: Criminal
- ▶ Workplace Violence: Assault

References

Gooch, G., & Williams, M. (2015). actus reus non facit reum nisi mens sit rea. In *A dictionary of law enforcement*. Oxford: Oxford University Press.

Gottschalk, P. (2018). Empirical study of convenience theory: A student elicitation on white-collar crime. *Deviant Behavior, 39*(6), 747–757.

Kivivuori, J., Savolainen, J., & Aaltonen, M. (2016). The revenge motive in delinquency: Prevalence and predictors. *Acta Sociologica, 59*(1), 69–84.

Los Angeles Police Department. (n.d.). *Why Young People Join Gangs*. Retrieved from http://www.lapdonline.org/get_informed/content_basic_view/23473

Maasberg, M., Warren, J., & Beebe N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. *2015 48th Hawaii International Conference on System Sciences (HICSS)*, HI, USA, pp. 3518–3526. https://doi.org/10.1109/HICSS.2015.423.

National Council on Alcoholism and Drug Dependence, Inc. (n.d.). Alcohol, Drugs and Crime. Retrieved from https://www.ncadd.org/about-addiction/alcohol-drugs-and-crime

National Safety Council. (2018). *Is Your Workplace Prone to Violence?* Retrieved from https://www.nsc.org/work-safety/safety-topics/workplace-violence

U.S. Department of Health and Human Services. (n.d.). *What is the U.S. Opioid Epidemic?* Retrieved from https://www.hhs.gov/opioids/about-the-epidemic/index.html

Vaughan, J. (2018). MS-13 resurgence: Immigration enforcement needed to take back our streets. https://cis.org/Report/MS13-Resurgence-Immigration-Enforcement-Needed-Take-Back-Our-Streets

Violence Policy Center. (2018). American Roulette: Murder-Suicide in the United States. Retrieved from http://vpc.org/studies/amroul2018.pdf

Yates, G., & Bass, C. (2017). The perpetrators of medical child abuse (Munchausen Syndrome by Proxy) – A systematic review of 796 cases. *Child Abuse & Neglect, 72*, 45–53.

Further Reading

Cullen, F., Agnew, R. & Wilcox, P. (2014). *Criminological Theory: Past to Present*. Oxford University Press.

Fox, J., Levin, J. & Quinet, K. (2018). *The Will to Kill: Making Sense of Senseless Murder*. Sage Publications.

Webber, C. (2019). *Psychology and Crime*. Sage Publications.

Criminals: Suggestions to Improve Security Procedures

Harald Haelterman
Faculty of Law and Criminology – Department of Criminology, Criminal Law and Social Law, Ghent University, Ghent, Belgium

Keywords
Security procedures · Controls · Procedural change · Crime script analysis

Definition

Procedure: a formal or official order or way of doing things – a series of actions that need to be completed in order to achieve something.

Introduction

Security procedures are considered a critical component of an organization's overall security program (Dunham 2018). They provide guidance on how to implement, enable, and enforce existing security controls and on how to execute security-relevant business processes in a consistent and concerted manner (ibid.). At the same time, they are to be considered controls in their own right. Same as other components of a security program, they require constant fine-tuning in order to remain effective and efficient over time. This entry highlights a number of triggers or incentives for organizations to upgrade existing security procedures or to implement new ones. It further positions script analysis as a promising tool to ensure that controls and procedures remain effective and fit for purpose.

Security Procedures in the Overall Control Framework

Procedures are defined as formal or official ways of doing things or as series of actions that need to be completed in order to achieve something (Hornby 1995). In the field of security,

this can be the proper implementation or enforcement of existing security controls or the execution of security-relevant business processes (Dunham 2018). Security procedures are developed and introduced in order to ensure that these controls and processes are implemented, enabled, enforced, and executed in a consistent and concerted manner, providing a reasonable degree of assurance and predictability (ibid.). They build upon the organization's security policies and focus on guiding behavior toward a certain and desired end result (ibid.). On the other hand, they are to be considered controls in their own right. The introduction of rules or procedures intended to remove any ambiguity concerning the acceptability of conduct is considered an important strand of situational crime prevention and an effective means to remove potential excuses for nonconforming behavior on the part of those intended to obey them (Clarke 1997, p. 24).

The idea behind having appropriate security procedures in place is that whenever they are followed consistently by everyone in scope, a desired and expected outcome is to follow. This does not imply that procedures remain effective and efficient as the internal or external environment changes. Just as security policies should be reviewed and updated on a regular basis, existing security procedures require constant fine-tuning, and new procedures will need to be introduced if and when required (Dunham 2018).

Drivers for Procedural Change

Various developments or events trigger the need to have new security procedures established or existing ones reviewed. As Oliver and Wilson already noted back in 1972, "the changing scene in which security is practiced constantly brings new problems" (Oliver and Wilson 1972, p. ix). These may arise from new or changing threats, from legal and regulatory changes, from a quest for efficiency gains or the need to adapt defensive approaches to the modi operandi displayed by offenders.

It goes without saying that security controls and accompanying procedures will need to be established or revisited as *new security threats* are being recognized (Threat Assessment). These threats can emerge from new products or services being introduced (see, e.g., Clarke and Newman 2005); from political, economic, social, and technological developments taking place; or from new crime phenomena entering the scene. Rapid advances in technology and an ever-increasing dependency on information and communication systems alone, for example, have been responsible for reshaping the entire security industry and for introducing a wide variety of IT ("information technology") security measures in public and private organizations alike (Cybersecurity: Cybercrime and Prevention Strategies).

Changes to *legal and regulatory frameworks* are certainly among the most obvious triggers for organizations to introduce or upgrade security controls and procedures. These regulatory changes are often brought about by highly publicized incidents or events such as the Lockerbie bombing back in 1988, the cowardly attacks on the Madrid rail system in 2004, the liquid plot in 2006, or the recent terrorist attack on Brussels airport in 2016 (▶ Airport Security: Incidents that Changed Procedures). Other examples of incidents or events that served as catalysts for governments to impose new requirements to (listed) companies with regard to security, corporate governance, and internal control are the hijackings and subsequent attacks on the World Trade Center and the Pentagon on September 11, 2001; the early twenty-first-century economic and financial crisis; a series of corporate collapses; and a range of high-profile frauds, corruption, and accounting scandals (Alexander and Alexander 2002; Chtioui and Thiéry-Dubuisson 2011, pp. 289–290). In response to the 9/11 attacks alone, we have witnessed the introduction and further strengthening of a broad range of transborder security programs designed to protect international supply chains against acts of unlawful interference and imposing a variety of specific and binding security requirements upon operators in the industry (Haelterman 2009, p. 485; 2011, p. 390) (▶ Critical Infrastructure: Transportation Systems). In many cases the introduction of these

requirements went hand in hand with employers undertaking additional security efforts due to the perception of growing terrorist threats and to employees demanding improved security at the workplace (Alexander and Alexander 2002, pp. 148–149).

Procedural innovation may further be required when it is found that security procedures contradict procedures or requirements imposed by other functions or when interdependencies between existing controls have been overlooked. An often quoted example of *contradicting* or *competing procedural requirements* is that of a security department requiring guards to make sure that all external doors of a facility remain locked at all times versus the requirement imposed by the health and safety function to keep these doors unlocked in order not to obstruct escape routes in case of an evacuation (▶ Fire: Evacuation). Examples of *interdependencies* that may be overlooked are those between physical security measures and accompanying procedures. It is of little use, for example, to install an electronic access control system without having proper access control procedures in place (Haelterman 2009, p. 490), to install GPS ("Global Positioning System") or similar technology on vehicles transporting high-value goods without the necessary follow-up capabilities and procedures (ibid.), or to invest in a CCTV ("closed-circuit television") system without having monitoring procedures in place that are appropriate for its setup and design (Clarke 1997, p. 26) (▶ Physical Security: Video Surveillance).

Likewise, procedures may need to be reviewed when it turns out that procedural requirements overlap and result in a *duplication* of efforts or when they turn out to be *too costly* or *impractical* in one way or another. Cost and waste management constantly drive organizations to transform existing strategies and practices in an ongoing quest for efficiencies. The introduction of security measures in a business environment often requires a considerable financial investment and frequently results in additional costs and/or practical problems due to their impact on certain core processes (Haelterman 2011, p. 394). The introduction of cargo screening procedures in a transport and logistics environment, for example, delays (and adds costs to) the normal operating process (ibid.), and imposing mandatory security screening of job applicants clearly adds costs and complexity to a new employee selection and onboarding program (▶ Personnel Security: Best Practices). It is important, therefore, to always engage in an ex ante and periodic assessment and evaluation of the (financial, ethical, esthetical, and consequential) costs associated with introducing security measures and of the conditions that influence their effectiveness and efficiency (see also Haelterman 2009, 2011).

Last but not the least, procedures may require an upgrade as part of the "postmortem" activities of an actual security incident (Dunham 2018). When it shows from a detailed analysis of the *modus operandi* displayed by an offender that an existing control or procedure was either easily circumvented or turned out to be ineffective for some other reason, an upgrade is required. The next section positions script analysis as a promising tool to guide such analysis.

Tools for Upgrading Existing Controls and Procedures

While the need for establishing new procedures or for updating existing ones is sometimes triggered by events and developments that go beyond management control, this is by far not always the case. This final section positions script analysis as a useful analytical tool to help management upgrade existing security controls and procedures in reaction to a real-life or improvised security incident. Other tools worth exploring are BSA ("Behavior Sequence Analysis"), in which a quantitative method is applied to qualitative data in order to investigate the relationships between events and to anticipate and redirect potentially risky patterns of behavior (see, e.g., Taylor et al. 2017), as well as the use of virtual reality to study the crime commission process in more detail (see, e.g., van Gelder et al. 2016).

Crime Script Analysis

Derek Cornish (1994) was the first to adopt the script concept from cognitive science in support of situational crime prevention. This concept,

according to Cornish (Idem: 151), offers "a useful analytic tool for looking at behavioral routines in the service of rational, purposive, goal-oriented action" and fits in particularly well with the crime-specific orientation that is found in rational choice and allied approaches to crime control. A script-theoretic approach, yet according to Cornish (Idem: 160), "offers a way of generating, organizing and systematizing knowledge about the procedural aspects and procedural requirements of crime-commission." To (environmental) criminologists and crime analysts, script analysis provides opportunities for understanding the "step-by-step process that offenders have to go through in the commission of any crimes" (Leclerc and Wortley 2014, p. 6); and by providing a template to capture and describe each stage of that process, it further assists researchers and practitioners with identifying a broad scope of opportunities for situational interventions (ibid.).

In the fields of cognitive science and artificial intelligence, scripts have been positioned as one of the theoretical entities or knowledge structures that form the basis of human memory organization (Schank and Abelson 1977, p. 17). A script (as an "event schema") is defined as "a structure that describes appropriate sequences of events in a particular context" (Idem: 41; Leclerc and Wortley 2014, p. 6). Applied to the criminological domain, it represents the complete sequence of actions adopted prior to, during, and following the commission of a particular crime (Leclerc and Wortley 2014, p. 6). If we take the hypothetical example of a script representing a theft of cargo from a soft-sided trailer parked at an unsecured parking lot (see also Table 1), such script could provide detail on potential preparations made prior to the actual theft, on the entrance to the parking lot, on the selection of a trailer to hit upon, on the means of gaining access to the load, and on the actual commission of the theft (Haelterman 2016, p. 14). It could further provide detail on the offenders exiting the crime scene, as well as on any follow-up actions (ibid.).

Scripts can be developed from the perspective of the offender – as is the case in our hypothetical example – or from that of other actors or agents participating in the crime commission process (Haelterman 2016, p. 16). They can be turned into interpersonal scripts, providing detail on the interactions between the various parties involved (Idem: 17), and can be used to study successful, attempted, failed, or aborted crimes (see, e.g., Cornish 1994, p. 163).

Criminals: Suggestions to Improve Security Procedures, Table 1 Example of script "cargo theft from parked trailer". (Modified from Haelterman 2016, p. 14)

Script scene	Script action
Preparation	Steal a van or light truck to transport the stolen items
Preparation	Gather the necessary tools for breaking into the trailer
Entry	Enter unsecured parking lot
Precondition	Drive around in search for soft-sided trailers
Instrumental precondition	Select a soft-sided trailer to hit upon
Instrumental initiation	Approach selected trailer
Instrumental actualization	Cut hole into the tarpaulin to check the load
Instrumental actualization	Break seal/lock on the trailer back door
Doing	Off-load cargo from the trailer
Doing	Load cargo into the getaway vehicle
Exit	Exit parking lot
Aftermath	Offer stolen goods for sale on the black market

The value of script analysis to those tasked with developing and reviewing security controls is that it forces them to study the crime commission process in more detail with a potential to reveal information that may be missed during a more superficial assessment of a criminal event (Haelterman 2016, p. 19). It facilitates the identification of potential intervention points and provides guidance on where preventive measures can best be introduced (Cornish 1994, p. 164). Building upon our hypothetical example of cargo theft from a parked trailer, Table 2 provides some examples of controls that can potentially be mapped onto the script to prevent repeat victimization. Where these controls are missing, their introduction can be considered; and where they are in place but have been circumvented, it is

Criminals: Suggestions to Improve Security Procedures, Table 2 Preventing "cargo theft from parked trailer". (Modified from Haelterman 2016, p. 20)

Script action	Situational controls
Steal a van or light truck to transport the stolen items	Car alarms, ignition locks, steering locks, immobilizers
Gather the necessary tools for breaking into the trailer	Control markets for dual goods, random vehicle searches
Enter unsecured parking lot	Access controls and procedures, parking attendants, select secure parking facilities
Drive around in search for soft-sided trailers	Enhance visibility and natural surveillance, on-site patrolling, camera surveillance, raise awareness and informal social control
Select a soft-sided trailer to hit upon	Replace soft-sided trailers with hard-sided trailers
Approach selected trailer	Enhance visibility and natural surveillance, on-site patrolling, camera surveillance, raise awareness and informal social control
Cut hole into the tarpaulin to check the load	Intrusion detection, anti-slashing strips on soft-sided trailers
Break seal/lock on the trailer back door	Intrusion alarms, security seals, security locks, park trailers back-to-back or facing a wall or fence
Off-load cargo from the trailer	Enhance visibility and natural surveillance, on-site patrolling, camera surveillance, raise awareness and informal social control
Load cargo into the getaway vehicle	Enhance visibility and natural surveillance, on-site patrolling, camera surveillance, raise awareness and informal social control
Exit parking lot	Exit controls and procedures, exit searches
Sell stolen goods on the black market	Disrupt markets for stolen goods

worth assessing why they turned out to be ineffective.

Reactive, Proactive, and Hypothetical Scripting

Crime script analysis can be applied in a proactive, reactive, and hypothetical mode to identify control gaps and control deficiencies and to select the most appropriate controls and control improvements that will help to prevent (repeat) victimization (Haelterman 2016, p. 123). *Reactive scripting* refers to the application of script analysis in the aftermath of a criminal event (ibid.). *Proactive scripting*, on the other hand, refers to the development of crime scripts based on information retrieved elsewhere (e.g., shared within industry bodies, gathered from the press, from professional or academic literature, from seminars and networking activities, etc.) (Idem: 124). By means of developing and interpreting scripts in a proactive manner, those responsible for designing controls gain the ability to assess whether their own organization has the necessary safeguards in place to avoid becoming a next victim (ibid.). *Hypothetical scripting*, finally, refers to putting oneself in the mind of the offender and viewing the task of breaching existing controls from an offender perspective (Ekblom, quoted in Moreto and Clarke 2014, p. 216). The type of scripts derived from these thought experiments are referred to as *potential scripts*, describing hypothetical sequences of actions and highlighting the various tracks that an offender could follow to commit a crime (Borrion 2013, p. 4).

Conditions for Successful Scripting

As with any analytical tool, the value of script analysis will depend on the amount and quality of data that is being gathered and processed. The more detail that is available on the offender's (hierarchy of) goals, decisions, actions, and interactions with the environment and other agents, the more potential for successful interventions (Haelterman 2016, p. 129). It is a known fact, however, that crime scripts often suffer from fragmented and insufficiently detailed information

(see, e.g., Cornish 1994, p. 160; Gilmour 2014, p. 39). It is important, therefore, that crime commission is being addressed at the appropriate level of specificity during interviews and investigations in general and that sufficient attention is being paid to the quality of (internal) reporting (Cornish 1994, p. 167; Haelterman 2016, pp. 236–237).

Conclusion

Security procedures provide guidance on how to implement, enable, and enforce existing security controls and on how to execute security-relevant business processes in a consistent and concerted manner. At the same time, they are to be considered controls in their own right. Same as other components of a security program, they require constant fine-tuning. New procedures may need to be established, or existing ones reviewed, as new security threats are being recognized or as the external environment changes. Upgrades may further be required in a quest for efficiency gains or when existing controls and procedures turn out to be ineffective. This entry positions script analysis as a promising and pragmatic tool to help crime prevention practitioners break down the crime commission process with the aim to identify potential intervention points, to strengthen existing controls, or to introduce additional ones. The tool can be applied in a reactive mode to properly identify control gaps and control deficiencies following an incident or in a proactive or hypothetical mode to routinely test the effectiveness of an organization's security and control setup. As to embrace the full potential of script analysis, however, it is key to address crime commission at the appropriate level of specificity during interviews and investigations and to pay sufficient attention to the quality of (internal) reporting.

Cross-References

- ▶ Airport Security: Incidents that Changed Procedures
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Fire: Evacuation (Engineer Solutions)
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Video Surveillance, Equipment, and Training

References

Alexander, D. C., & Alexander, Y. (2002). *Terrorism and business. The impact of September 11, 2001*. Ardsley: Transnational Publishers.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science, 2*(6), 1–12.

Chtioui, T., & Thiéry-Dubuisson, S. (2011). Hard and soft controls: Mind the gap! *International Journal of Business, 16*(3), 289–302.

Clarke, R. V. (1997). Introduction. In R. V. Clarke (Ed.), *Situational crime prevention. Successful case studies* (2nd ed., pp. 1–44). New York: Harrow and Heston.

Clarke, R. V., & Newman, G. R. (Eds.). (2005). *Crime prevention studies volume 18: Designing out crime from products and systems*. Monsey: Criminal Justice Press.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime prevention studies* (Vol. 3, pp. 151–196). Monsey: Criminal Justice Press.

Dunham, R. (2018, March 14). Security procedures – How do they fit into my overall security documentation library? https://linfordco.com/blog/security-procedures/. Accessed 1 Dec 2018.

Gilmour, N. (2014). Understanding money laundering. A crime script approach. *The European Review of Organised Crime, 1*(2), 35–56.

Haelterman, H. (2009). Situational crime prevention and supply chain security: An ex ante consideration of preventive measures. *Journal of Applied Security Research, 4*, 483–500.

Haelterman, H. (2011). Re-thinking the cost of supply chain security. *Crime, Law and Social Change, 56*(4), 389–405.

Haelterman, H. (2016). *Crime script analysis. Preventing crimes against business*. London: Palgrave Macmillan.

Hornby, A. S. (1995). *Oxford advanced learner's dictionary of current English* (5th ed.). Oxford: Oxford University Press.

Leclerc, B., & Wortley, R. (2014). The reasoning criminal. Twenty-five years on. In B. Leclerc & R. Wortley (Eds.), *Cognition and crime. Offender decision making and script analyses* (pp. 1–11). New York: Routledge.

Moreto, W. D., & Clarke, R. V. (2014). Script analysis of the transnational illegal market in endangered species. In B. Leclerc & R. Wortley (Eds.), *Cognition and crime. Offender decision making and script analyses* (pp. 209–220). New York: Routledge.

Oliver, E., & Wilson, J. (1972). *Practical security in commerce and industry* (2nd ed.). New York/Toronto: Wiley.

Schank, R. C., & Abelson, R. P. (1977). *Scripts, plans, goals and understanding. An inquiry into human*

knowledge structures. Hillsdale: Lawrence Erlbaum Associates.
Taylor, O., Keatley, D. A., & Clarke, D. D. (2017). A behavior sequence analysis of perceptions of alcohol-related violence surrounding drinking establishments. *Journal of Interpersonal Violence.* https://doi.org/10.1177/0886260517702490.
van Gelder, J.-L., Nee, C., Otte, M., Demetriou, A., van Sintemaartensdijk, I., & van Prooijen, J.-W. (2016). Virtual burglary: Exploring the potential of virtual reality to study burglary in action. *Journal of Research in Crime and Delinquency.* https://doi.org/10.1177/0022427816663997.

Further Reading

Abbott, A. (1995). Sequence analysis: New methods for old ideas. *Annual Review of Psychology, 21*, 93–113.

Criminals: Terrorists

James M. Duggan and James J. F. Forest
Center for Terrorism and Security Studies,
University of Massachusetts Lowell,
Lowell, MA, USA

Keywords
Terrorist · Extremist perpetrator · Radicalized criminal

Definition

Terrorists are criminals who commit or directly support acts of violence in order to achieve some type of sociopolitical objectives.

Introduction

This chapter examines the groups and individuals who commit or directly support acts of terrorism. The phenomenon of terrorism itself will be covered in other chapters of this volume, including ▶ "Terrorism: Domestic" and ▶ "Terrorism: International". Terrorists are widely considered a distinct type of criminals. They consciously choose to kill, maim and destroy, and also routinely engage in money laundering, theft, fraud, extortion, smuggling (including drugs, weapons, and humans), kidnapping, bank robbery, and many other kinds of criminal activity. But terrorists generally loathe being labeled as ordinary criminals, preferring to use labels like "freedom fighters" or in the case of some religious groups, "holy warriors." And as described later in this chapter, terrorism is also viewed as a type of political violence.

Generally speaking, terrorists are not crazed killers but instead are usually rational actors who employ terrorist tactics in a calculated effort to magnify their relatively meager resources, draw attention to their plight, and garner support for their cause (Hoffman 2017). Further, the strategic goal of most terrorists is not to kill a lot of people but rather to kill a relatively few and strike fear in the hearts of many, in order to coerce the behavior of a society and its government in ways the terrorists feel will help them achieve their political or social objectives (Forest 2018).

This underscores the communicative aspect of their crimes; unlike many other violent criminals (who tend to avoid the media), terrorists often claim responsibility for attacks and try to justify their violence through their ideology, an articulation of their grievances and goals. There are many different ideological categories of terrorism, including ethnonationalist, left-wing, right-wing, and religious. Within each of these categories, there is a wide spectrum of groups and goals. For example, the category of religious terrorism includes Salafi-Jihadist groups like Al-Qaeda and Islamic State, Shiite militia groups like Hezbollah, Christian antiabortion extremists like the Army of God, and even the Japanese Buddhist cult Aum Shinrikyo. There are also terrorists who use violence on behalf of extreme goals related to environmental protection or animal rights. Each of these ideological categories will be described in this chapter, along with some examples of relevant individuals and groups.

Beyond the ideological dimension, there are also many other differences among terrorists. To begin with, researchers have sought in vain for common attributes among terrorists, but the evidence shows that they can be any age, ethnicity, or religion and from any socioeconomic or

educational background (Hoffman 2017; Forest 2018). Both men and women have been terrorists, even suicide bombers (Hoffman 2017; Forest 2018). Some terrorists may have signs of mental illness, but researchers have found nothing that would separate them from other mentally ill individuals who engage in non-terrorist criminal activity (Horgan 2005; McCauley 2007; Corner and Gill 2015). There are also many different roles an individual could play within a terrorist group, from explosive expert to budget manager, logistician, driver, propagandist, and many more (Horgan 2009; Forest 2018). This complicates matters for law enforcement and court systems when trying to prosecute individuals accused of terrorist activity. For example, should a terrorist group's bomb-maker be treated the same as another member whose role was financial management or document forgery? These and other issues will be addressed in the chapter ▶ "Investigations: Terrorism".

Overall, as this chapter will illustrate, identifying and explaining who is (or is not) a terrorist is not as easy or straightforward as some politicians or media pundits would have us believe. The chapter begins with a brief discussion about the definitional challenges of terrorism and then will review the ideological categories that have motivated most terrorists around the world. Attempts to identify a common demographic profile of terrorists will be reviewed, and examples of particularly prominent terrorists will be used to illustrate the diversity within this category of criminals. Finally, the chapter will conclude with some thoughts about the future of research on terrorists and implications for security and emergency management.

Conceptualizing Terrorism

Terrorism is an extremely complex phenomenon that is open to interpretation and subject to competing opinions among researchers. Consistent with this complexity, there are many definitions of terrorism, not only among individual researchers but also among the various government agencies that contribute to counterterrorism efforts within the USA. For instance, the US Department of State employs the definition provided by Section 2656f(d) of Title 22 of the United States Code, which defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents," and the Department of Justice defines terrorism as "the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (Hoffman 2017). Yet another definition is offered by the Global Terrorism Database (GTD), a tool frequently used by terrorism researchers and policymakers, which defines terrorism as "the threatened or actual use of illegal force and violence by non-state actors to attain a political, economic, religious, or social goal through fear, coercion, or intimidation" (Crenshaw and Lafree 2017, p. 23). In general, the diversity of definitions used by scholars and government agencies can be problematic when conducting terrorism research or investigations.

Despite the lack of clarity presented by the various definitions, there are some characteristics of terrorism that are generally accepted by researchers. One of these characteristics is that the violence targets noncombatants, which includes off-duty military and law enforcement, as well as civilians, all of which violates international humanitarian law (Hoffman 2017). In addition, the targeted noncombatant victims of the attack are not the true intended victims of the attack but rather are victimized in order to inflict psychological trauma and "terrorize" the greater society (Horgan 2009). The fear and "terror" inflicted on society are driven in part by the apparent randomness of the attacks and the ferocity of the methods employed, such as beheading hostages and killing women and children (Crenshaw and Lafree 2017).

In addition to being a form of criminal activity that causes psychological trauma, terrorism is also viewed as a type of *political violence* (along with insurgency, guerilla warfare, rebellion, etc.). Terrorists use acts of violence as a way to achieve some type of political goals. Some may want

to overthrow an established government (the classic definition of insurgency), like the Taliban, Al-Qaeda in the Arabian Peninsula, and the Islamic State (Crenshaw and Lafree 2017). Others want the power to control a specific territory (like Hamas or other Palestinian groups) or perhaps even establish an ethnically homogenous "homeland" (like the Basque group ETA in northern Spain). Even religious terrorists are seeking to achieve some kind of political objectives, from establishing an Islamist Caliphate in the Middle East to stopping the practice of abortions in the USA (Forest 2018). Thus, understanding the motives, goals, and objectives of terrorists is necessary for researchers, policymakers, and practitioners.

Motivations of Terrorists

Perhaps the most distinguishing feature of terrorists, compared to other violent criminals, is the nature of their motivations. While other terrorists may carry out acts of violence for profit, revenge, control of drug trafficking routes, and so forth, terrorists articulate their motivations in a broad range of ideological statements. In fact, terrorist groups over the past 120 years have shown a keen interest in shaping perceptions about their activities and efforts to justify their criminal activities as necessary for achieving some preferable future (Forest 2018). There are many categories of ideologies, including ethnonationalist/separatist, left-wing, right-wing, and religious, each of which will be briefly explained below.

The most distinguishing aspect of ethnonationalist/separatist groups is their focus on physical and political geography. The ideology of terrorists in this category is driven by their desire to wrest control of a geographic area from the government in order to establish an independent state for those of a particular ethnicity, like the Chechens in Russia, Kurds in Turkey, Basques in Spain, or Tamils in Sri Lanka. And unlike the ideologies of other terrorist groups, the membership of ethnonationalist/separatist groups is limited by their ethnicity (Forest 2018).

Left-wing terrorists are driven by a utopian vision of a society that provides greater equality through the implementation of a communist government (Forest 2018). Often referred to as Communist, Maoist, or Marxist-Leninist, the ideology of left-wing terrorists is often consistent with Russian revolutionaries who galvanized the working masses to revolt against the government. Left-wing terrorists incite class warfare but are willing to allow anyone to join their cause. While not as common today, left-wing terrorist movements were prominent during the 1960s through 1980s, including the Red Army Faction (RAF) in West Germany, the Red Brigades in Italy, the Weather Underground in the USA, and Sendero Luminoso in Peru.

Right-wing terrorists are often described as either revolutionary or reactionary; the former usually target the government, while the latter may focus on countering the efforts of left-wing movements or threat to the status quo (Forest 2018). For example, the Ku Klux Klan (KKK) became a well-known right-wing terrorist movement in the USA that blocked social reconstruction policies and civil rights in the south. Many right-wing terrorists are anti-leftist, anti-liberal, religiously extreme, anti-government (e.g., the sovereign citizen movement in the USA), anti-gun control, or paramilitary/militia in nature, and some are also racial supremacists (including the Aryan Nations, The Order, Hammerskin Nation, and the American Front), targeting the members of minority groups whom they perceive as a threat.

And finally, the largest and most prominent category of terrorist ideologies today is religious. The past half-century has seen the rise of myriad Christian, Jewish, Sikh, Buddhist, Hindu, and Islamist terrorist groups, all of whom are inspired by the belief that terrorism is necessary to achieve (their interpretation of) God's will and that the truly pious terrorist is at war with those whose destiny is eternal damnation. From Al-Qaeda and the Islamic State to Hamas (in Israel), Hezbollah (in Lebanon), or the Army of God (a violent anti-abortion movement in the USA), religious terrorists have much in common. More than other categories of terrorists, the religious extremists

are absolutist (you are either with them or the enemy, there are no innocent bystanders) and supremacist (their interpretation of the faith is the one and only truth). This combination often means a negotiated compromise to address their grievances is impossible.

This category also includes some of the only examples of terrorists who have engaged in attacks using weapons of mass destruction. For example, Aum Shinrikyo was a Japanese religious cult that integrated elements of esoteric Buddhism, Hinduism, messianic Christianity, and apocalyptic prophesies. In 1995 Aum Shinrikyo launched a sarin nerve agent attack on a Tokyo subway that left a dozen dead and more than 3000 injured. Another religious cult, the Rajneeshes, used salmonella to poison a local population in the state of Oregon. And most recently, the Sunni jihadist group Islamic State used chemical weapons (including chlorine, phosphine, and mustard agents) dozens of times in Iraq and Syria over a 4-year period. Of all the terrorist groups currently threatening civil societies worldwide, religious terrorists account for an overwhelming majority.

These various ideologies shape a terrorist group's recruitment efforts, tactics, and targets. For example, left-wing terrorists typically target government buildings and centers of capitalism, as well as symbols of authority and power, such as police stations, politicians, industry, and military facilities. Meanwhile, animal rights extremists will target animal research laboratories and the businesses that finance them, and right-wing groups will target members of a minority population or perhaps a synagogue. Similarly, an attack against a particular target will likely indicate the type of ideology motivating the group or individual responsible for that attack.

Throughout these ideological categories, some common themes can be identified. First, the grievances articulated by the terrorists often include some complaint about government legitimacy (or lack thereof). According to Ted Robert Gurr's theory of relative deprivation, (Gurr 2016 [1970]), the risk of political violence in a country rises as the perceived legitimacy of a government declines. Contributing factors to perceived illegitimacy of a government include corruption, repression, indiscriminate violence, and incompetence. Sometimes, a terrorist group will carry out violent attacks in order to provoke a violent overreaction by the government in order to negatively impact the legitimacy of the regime and generate more support for the terrorist group.

Other grievances that could motivate an individual toward terrorism include structural disadvantages that exclude particular segments of a society from economic, educational, or political opportunities or the provision of social services. These contribute to a gap between an individual's aspirations for a better life and opportunities to achieve those aspirations, generating significant frustrations. However, the research also indicates that the most poverty-stricken regions of the world are no more likely to spawn terrorists than a wealthy country. In fact, there are many impoverished areas of the world that have produced no terrorists, while a significant number of today's jihadists and right-wing terrorists were raised in affluent neighborhoods, went to college, and even became engineers and physicians (Forest 2018). The broad range of personal grievances and frustrations, in turn, help explain why the majority of terrorist attacks worldwide are domestically oriented – that is, they are perpetrated by citizens or residents of the country in which the attack occurs. Despite what today's overhyped media coverage and political rhetoric about international terrorism suggest, domestic contexts have always had a far more powerful impact on motivating a person toward terrorist activity.

Another common dimension among many religious, ethnonationalist, and right-wing terrorists is "othering," loosely defined as identifying a specific population or subgroup (e.g., Jews, Protestant loyalists, blacks, "infidels," etc.) as the primary source of evil. Adherents of right-wing terrorism are driven by a particularly strong sense of "othering" that dehumanizes those they perceive of as their enemy, while the "othering" component of religious terrorism is even more radical and contributes to their zero-sum worldview.

Overall, because terrorism is a highly contextual phenomena, we must consider the

socioeconomic, political, and cultural environment that contributed to the motives of an individual to engage in terrorist activity. When examining incidents of terrorism, we must remain cognizant of the fact that terrorism does not occur in a vacuum; there is a constant interplay of myriad socioeconomic and political factors, as well as interpersonal relationships and group dynamics that provide for the environment in which individuals make rational choices. Further, it is important to remember that individuals from virtually all walks of life have been drawn into terrorist activity.

Demographics

While motivations may be the most central element separating terrorists from other kinds of violent criminals, some politicians and media pundits have attempted to portray a certain type of individual as most prone to being a terrorist. In today's politically charged environment, personal characteristics such as young, Arab, male, and immigrant have been misappropriated by some as proxy representations of the terrorist threat within the USA. And yet, nearly five decades of research by thousands of scientists and scholars have found no evidence of any common personal traits or characteristics that would help us predict the likely risk of involvement and engagement in terrorist activity (Horgan 2005). Instead of a common terrorist profile, the evidence reinforces the point made earlier in this chapter: individuals consciously choose whether to perpetrate or support acts of terrorism. Further, individuals from virtually *any* background can choose to engage in terrorist activity.

Some researchers have questioned whether mental illness might play a role, arguing that surely only crazy people would be able to justify to themselves the horrific crimes inflicted by terrorists upon innocent civilians (McCauley 2007). And yet, empirical research indicates that terrorists are rarely mad, very few suffer from personality disorders, and there is little evidence that terrorists are suffering from psychopathology (Hoffman 2017; McCauley 2007; Silke 2004). In fact, research has shown that terrorist organizations most often shun those who display any signs of mental illness, unless there is a specific tactical use for them – for instance, the Provisional IRA, or PIRA, employed the mentally ill to beat up members who got out of line but would not deploy them in an ordinary operational capacity (Horgan 2009).

One exception to this body of research may be found among terrorists who carry out attacks without the direct involvement of an established organization – the so-called "lone wolf" phenomenon. For example, a recent study (Corner and Gill 2015) suggests that terrorists who are not members of an organization are more likely to suffer from mental illness than members of the broader population. Further, they found that lone actor terrorists were significantly more likely to suffer mental illness than terrorists who were members of an established group. More research in this area is needed, but the study reflects an important modern challenge for security and emergency management professionals: how to respond to the lone actor terrorist.

Forest (2018) prefers the term "do-it-yourself" terrorists rather than "lone actor" or "lone wolf," as true lone actors are extremely rare. In this description, the do-it-yourself terrorist is one who has not had any direct operational support or training from an established terrorist group but was simply inspired to plan and execute a terrorist attack entirely on their own. While a terrorist group's ideology may provide them with a perceived justification for the act of violence, the individual chooses the target, weapons, and timing for the attack. During the late 1880s through the early 1900s, a wave of anarchists in Europe and the USA were the most prominent form of do-it-yourself terrorism, but more recent examples in the USA include the 1995 bombing of the Murrah Federal Building in Oklahoma City by Timothy McVeigh and the 1996 bombing of the Atlanta Olympics by Eric Rudolph, both of whom are considered right-wing terrorists in the research literature. And the last two decades have seen the rise of the do-it-yourself jihadists, inspired by the leaders of Al-Qaeda or the Islamic State to carry out terrorist attacks in Europe and

the USA. Some well-known examples include Nidal Hasan's attack at Fort Hood in 2009, the attempted attack against the New York subway by Najibullah Zazi and two of his friends that same year, the Tsarnaev brothers' attack against the Boston Marathon in 2013, and the mass shooting at an Orlando nightclub by Omar Mateen in 2016. The diversity of backgrounds and motivations among do-it-yourself terrorists reinforces the central fact that a common "terrorist profile" is inherently elusive. As a result, the question of who becomes a terrorist and why can only be answered by analysis that includes a broad range of contextual factors and influencers.

Terrorist Methods

Many kinds of crimes have been considered acts of terrorism when perpetrated by individuals pursuing some kind of sociopolitical agenda, as described above. One of the most common forms of terrorism has involved bombings against a wide range of targets, from public transportation to hotels, government buildings, and marketplaces. The bombs used in these attacks vary widely in size and sophistication, from the donkey cart, gunpowder, and shrapnel used by the anarchist Mario Buda in the 1920 Wall Street bombing to the two backpack pressure cooker bombs used by the Tsarnaev brothers in the 2013 Boston Marathon attack. Recently the highly unstable chemical explosive triacetone triperoxide (TATP) has been used in several jihadist terrorist attacks including the July 2005 bombing of the London Underground, the 2015 Paris attacks, the 2016 Brussels attack, and the 2017 Manchester attack. Since the introduction of suicide bombers by the Lebanese terrorist group Hezbollah in the early 1980s, there has been a global proliferation of this distinct method of delivering the explosives to the target (Hoffman 2017; Forest 2018). While the ethnonationalist group Tamil Tigers in Sri Lanka were the world's leading suicide bombers during the 1990s, we have since seen a global proliferation of this tactic involving mostly jihadist groups from Nigeria and Somalia to Pakistan and Afghanistan. Some of these groups have even deployed women and young children as suicide bombers (Forest 2018).

Beyond explosives, terrorist attacks have included a variety of other weapons, as demonstrated by the 2017 knife attack at London Bridge, ramming vehicles into crowds (e.g., Nice, 2016, and New York City, 2017) or intentionally crashing commercial airplanes into buildings (September 11, 2001). Terrorists have also engaged in kidnapping and hostage-taking for over a half-century, sometimes to bargain for policy concessions or an exchange of prisoners (e.g., the Red Army Faction during the 1970s) but increasingly to demand sizable monetary ransoms (e.g., the Abu Sayyaf Group and Al-Qaeda in the Islamic Maghreb, among several others). In Iraq and Syria, terrorists have posted videos online showing them beheading a number of western hostages as a warning to their enemies. This reflects one of the most important factors that distinguish acts of terrorism from other criminal acts – taking credit for the violence is part of the communicative strategy of terrorism. Today, terrorists used video cameras and social media to amplify the impact of their attacks as a way of generating more fear among the general public, in the belief that this will help them achieve the sociopolitical goals of their terrorist movement.

Conclusion

Obviously, nobody is born to be a criminal or terrorist. Terrorism is a type of deviant criminal behavior that is learned and can be motivated by a broad range of goals, contexts, and individuals. Much of the research on terrorist motivations has focused on an individual's perceptions, like "perceived legitimacy of the regime," "perceived threat," or "perceived opportunities." This underscores the simple fact that virtually anyone – under the right conditions – can become convinced to perpetrate or support acts of terrorism. Further, in addition to the impact of their surrounding contextual factors (political, socioeconomic, etc.), an individual's decision to engage in terrorism is influenced by friends, colleagues, terrorist group leaders, radical clerics, or even family members.

Terrorists are a distinct subcategory of criminals, defined by the sociopolitical nature of their motivations, and they engage in much more than just violent forms of criminality, to include drug smuggling, money laundering, theft, kidnapping, and much more. Security policies and strategies to combat terrorism require a broad range of intelligence and law enforcement actions as well as relevant socioeconomic policies that address the underlying contextual factors motivating the terrorists.

Cross-References

- ▶ Investigations: Terrorism
- ▶ Terrorism: Domestic
- ▶ Terrorism: International

References

Corner, E., & Gill, P. (2015). A false dichotomy? Mental illness and lone actor terrorism. *Law and Human Behavior, 39*(1), 23–34.

Crenshaw, M., & Lafree, G. (2017). *Countering terrorism*. Washington, DC: Brookings Institution Press.

Forest, J. (2018). *The terrorism lectures* (3rd ed.). Santa Ana: Nortia Press.

Gurr, T. (2016). *Why men rebel: 40th anniversary edition*. New York: Routledge. [originally published in 1970].

Hoffman, B. (2017). *Inside terrorism* (3rd ed.). New York: Columbia University Press.

Horgan, J. (2005). The social and psychological characteristics of terrorism and terrorists. In T. Bjorgo (Ed.), *Root causes of terrorism: Myths, realities and ways forward*. London: Routledge.

Horgan, J. (2009). *Walking away from terrorism: Accounts of disengagement from radical and extremist movements*. New York: Routledge.

McCauley, C. (2007). Psychological issues in understanding terrorism and response to terrorism. In C. Stout (Ed.), *Psychology of terrorism: Coping with the continuing threat*. Westport: Praeger.

Silke, A. (2004). An introduction to terrorism research. In A. Silke (Ed.), *Research on terrorism: Trends, achievements and failures*. London: Frank Cass.

Further Reading

Abrahms, M. (2008). What terrorists really want: Terrorist motives and counterterrorism strategy. *International Security, 32*(4), 78–105.

Forest, J. (2018). *The terrorism lectures* (3rd ed.). Santa Ana: Nortia Press.

Hoffman, B. (2017). *Inside terrorism* (3rd ed.). New York: Columbia University Press.

Criminals: White-Collar Crimes

Zakir Gul
Criminal Justice Department, State University of New York (SUNY), Plattsburgh, NY, USA

Keywords

Crime · Criminal · White-collar crime · White-collar criminal

Definition

The Federal Bureau of Investigation (FBI 2019; see chapter ▶ "Investigations: Criminal" in this encyclopedia) defines white-collar criminals as business and government professionals who commit crimes that are "characterized by deceit, concealment, or violation of trust and are not dependent on the application or threat of physical force or violence" and have a financial motivation rooted in the desire "to obtain or avoid losing money, property, or services or to secure a personal or business advantage."

Introduction

The terms *white-collar criminal* and *white-collar crime* have been discussed conceptually and theoretically since Edwin H. Sutherland coined the terms 80 years ago. The widely accepted literature in criminology held that crimes were committed by people from low socioeconomic communities or by people with psychological or biological problems, making any other possibility a radical concept at least then. Over the years, the definition of what constitutes white-collar crime has evolved and took new forms.

White-collar criminals tend to be wealthy middle- or upper-class men who are well-educated, employed, respected and trusted, nonviolent, with no prior criminal or disciplinary record, and commit crime in a legal corporate or professional setting mainly for financial and material gain. White-

collar crime, whether in the past or today, can have serious consequences for and impact on society, individuals, institutions, and the environment. With a single act, a white-collar criminal, whether an individual or corporation, can harm and victimize (directly or indirectly) many people financially, physically, psychologically, and sociologically. This crime can financially impact the society more than all blue collar crimes (see chapter ▶ "Criminals: Blue-Collar Crimes" in this encyclopedia) combined. For example, a white-collar criminal engaged in a Ponzi scheme caused investors in the scheme to lose $65 billion on paper (Fishman 2011) and a total of $90 billion in cash and on paper (Memmott 2011). After the leader of the scheme confessed to the crime, his son (Fishman 2011) and some of the investors (Cohen et al. 2017) committed suicide. In some other Ponzi-scheme cases, the perpetrators killed family members before taking their own lives (Saxby and Anil 2012).

Companies may inflict financial harm with their actions such as bankrupting and stealing pensions on the society. Further, they can also give physical harm that may affect the health and lives of the people. Pharmaceutical and food industries are just two examples that are being exploited by the corporations. Many victims of white-collar crime, however, may not even be aware that they are being victimized because the perpetrator is perceived as being honest (Cullen et al. 2009), trustworthy (Friedrichs 2010; Shapiro 1990), respected, and privileged (Shover and Wright 2001). White-collar criminals succeed and are able to conceal their illegal action by winning the trust and respect of their victims.

This chapter begins with describing the demographics and characteristics of white-collar criminals. It continues with the sections of theories and types and forms of white-collar crime. Finally, the impact and consequences of a white-collar criminality are discussed before the conclusion section.

Demographics

White-collar criminals typically are males in their 40s and 50s who have a middle- or upper-class socioeconomic status (ACFE 2018; Gottschalk 2014; Friedrichs 2010; Wheeler et al. 1988). White-collar criminals usually are *male* (Sutherland 1940; Wheeler et al. 1988; Blickle et al. 2006; Daly 1989). In one study, the majority (69%) of the occupational fraudsters were found to be males (Association of Certified Fraud Examiners [ACFE] 2018). One explanation for females as not being many white-collar criminals is the less opportunity of females due to some gender segregation and inequalities in the workplace (Benson and Gottschalk 2015). Daly (1989, pp. 789–790) found that "men's white-collar crimes were both petty and major, but almost all the women's [crimes] were petty." Daley noted that "although half or more of the employed men were managerial or professional workers, most employed women were clerical workers." Daley also found that female white-collar criminals were younger and had a lower level of education compared to male white-collar criminals.

Unlike blue-collar criminals, white-collar criminals tend to be *well educated* (Ragatz et al. 2012; Wheeler et al. 1988). A recent study found that 76% of the occupational fraudsters had some postgraduate education or had earned a degree from a university (ACFE 2018). White-collar criminals also are employed, homeowners, and generally *wealthier* than common criminals (Gottschalk 2014; Wheeler et al. 1988).

White-collar criminals usually are *middle-aged* and *older* than conventional criminals (Gottschalk 2014; Friedrichs 2010; Wheeler et al. 1988). ACFE (2018) reports that the majority (61%) of the occupational fraudsters are between the ages of 36 and 55 (19% at ages 36 to 40; 19% at ages 41 to 45; 14% at ages 46 to 50; 9% at ages 51 to 55), whereas only 5% of the offenders are under the age of 26. Further, 10% of the perpetrators are between the ages of 26 and 30; 15% of them are between the ages of 31 and 35. However, even though the age group of 56 and older makes up only 9% of the study sample, it is responsible for the largest median losses (56 and older ages for $ 835,000 compared with 30 or younger ages for $ 63,000).

Characteristics

White-collar criminals have specific qualities that aid them in committing crime. First, they are highly *trusted* individuals. Exploitation of this trust is at the core of their misdeeds, and it is what enables white-collar criminals "to rob without violence and burgle without trespass" (Shapiro 1990, p. 346). Some scholars, therefore, refer to white-collar criminals as *trusted criminals* (Friedrichs 2010) and their crimes as *crimes of trust* (Menard et al. 2011).

White-collar criminals are *respected*. They are "respectable or at least respected business and professional men" (Sutherland 1940, p. 1) who exploit this respectability. This respectability also can arise from factors such as moral integrity, a legitimate position or occupation, or an outward appearance of acceptable or superior status (Friedrichs 2010). Respectability can prompt people to trust white-collar criminals, thereby making it easier to engage in illegal activity.

White-collar criminals usually are *first-time offenders*, meaning that they do not have a prior record of criminal background, or employment-related disciplinary actions. ACFE (2018) reports that the vast majority (96%) of the perpetrators were not previously convicted of a fraud-related offense. In the same vein, the majority (85%) of the perpetrators were never punished administratively or terminated for fraud-related conduct before, either.

White-collar criminals can be *charismatic*. White-collar criminals, particularly those in leadership positions, have been known to use their charisma to commit white-collar crime (Bucy et al. 2008). For example, if the followers of a charismatic leader believe in their leader, the followers might choose loyalty over honesty, or the followers may feel powerless to question or confront the leader and therefore simply do what they are told to do.

White-collar criminals usually are *nonviolent* (Friedrichs 2010). Although many white-collar crimes have led to serious physical harm or death to some of the people involved, the perpetrators' use of violence against those victims is not believed to have been directly inflicted or intentional (Friedrichs 2010). White-collar crime, therefore, is viewed as a nonviolent crime. In such cases, the intent of the crime was not to injure or kill but to reap economic benefits or occupational success in a legitimate occupational context. Some researchers believe that the unintended injuries and deaths are inevitable side effects (Benson and Simpson 2009) or outcomes resulting from acts of inadvertence, omission, and indifference (Geis 1972).

White-collar criminals may, however, apply to violence to deceive people and cover their white-collar criminal activity. This approach led to the coinage of the concept known as "red-collar criminals" (Perri 2016). Red-collar criminals engage in violence to silence people "who are in a position to detect and/or disclose their fraud schemes: hence the name fraud detection homicide describing the motive to classify the murder" (p. 62).

Theories and Motives

Some of the theoretical approaches that give explanations for the motives of white-collar criminals are presented in this section. Given the complex and multifaceted nature of white-collar crime, no "single theory or explanation can comprehensively explain all forms or nuances" (Friedrichs 2010, p. 247), but each theory covers some part of the phenomenon.

One common motive for white-collar criminal is *greed* (Bucy et al. 2008; see chapter ▶ "Criminals: Motives" in this encyclopedia). This greed often is driven by the desire to acquire monetary and/or financial benefits and gains. Bucy and her colleagues (Bucy et al. 2008) found that greed has been the primary motive for white-collar criminals, especially for persons in leadership positions. Fear of failure and fear of losing one's job or lifestyle also motivate people to engage in white-collar crimes (Bucy et al. 2008, p. 407).

Sutherland explained the acts of white-collar criminals with his general theory of differential association (Sutherland 1940, 1945). Contrary to a major group of approaches popular during the late 1930s, Sutherland claimed that the actions of

white-collar criminals were "not correlated with poverty or the psychopathic and sociopathic conditions associated with poverty" (Sutherland 1940, p. 2). Rather, Sutherland argued, white-collar criminals were from the upper-class, were respected and wealthy, and learned about crime through direct or indirect associations with other criminals, and when the situation is considered as more favorable than unfavorable to commit the crime, white-collar criminals commit their crimes (Sutherland 1945).

Control theories help to explain some of the actions of white-collar criminals. Personality traits such as "low self-control" (Piquero et al. 2008) or the "desire for control" (Piquero et al. 2005) can help explain why some people commit crimes. Blickle et al. (2006), for example, found that high-ranking white-collar criminals have low behavioral self-control, high hedonism, high narcissism, and high conscientiousness.

White-collar criminals commit crime because they do not see themselves as criminals and deny their guilt, using inner justifications to do so (Cressey 1953; Benson 1985; Dhami 2007; Sykes and Matza 1957). White-collar criminals do not perceive their actions as criminal; therefore, they find ways to neutralize any feelings of apprehension, justify what they plan to do (Sykes and Matza 1957; Cressey 1953), commit the crime confidently, and deny their guilt (Cressey 1953; Benson 1985). For example, some white-collar criminals see their acts of embezzlement as borrowing from others or a legitimate response to being treated unjustly by their employer (Cressey 1953; see chapters ▶ "Retail Security: Employee Theft" and ▶ "Investigations: Employee Theft of Employer Property" in this encyclopedia). Other white-collar criminals justify their actions by saying that what they did not harm anyone (Dhami 2007) or that they had been set up and were wrongfully convicted or that their actions were justified because everyone was doing the same thing (Benson 1985).

Like control theories, rational choice theories help to explain why white-collar criminals engage in illegal activities. From the perspective of rational choice theories, white-collar criminals calculate their gains and losses before committing their crime (Paternoster and Simpson 1996). A white-collar criminal's decision about whether or not to commit a crime involves the "balancing of both the costs and benefits of offending" and the person's "*perceived* or subjective expectations of reward and cost" (Paternoster and Simpson 1996, p. 553).

Some opportunity theories can be used to explain the actions of white-collar criminals (Benson and Simpson 2009; Bucy et al. 2008). Certain conditions provide an attractive opportunity for a rational perpetrator to commit a white-collar crime. In other words, if the opportunity does not exist, then no crime will be committed. Opportunity theories also hold that regardless of how strong the perpetrator's motivation is to commit a white-collar crime, without the opportunity to act on that motivation, a crime will not be committed (Coleman 1987). Coleman (1987) also connected the opportunity to commit a white-collar crime to cultural influence – namely, the *culture of competition*, which is a natural part of a capitalist society. In such a competitive culture, some white-collar criminals will have more opportunities than other white-collar criminals to commit a crime.

Anomie theory also helps to explain the motives of white-collar criminals. The theory holds that while someone may have socially acceptable and legitimate goals, the absence of any legitimate means to reach those goals leads to deviant behavior. Schoepfer and Piquero (2006), for example, have applied anomie theory to explain embezzlement.

Types and Forms

While classifications of different types of *criminals* do exist in the literature, the classification of white-collar criminal is not among them. The white-collar crime literature focuses more appropriately on *criminality* (i.e., conduct, behavior) rather than on *criminals* (i.e., people). In this regard, one of the most comprehensive typology for white-collar crime is the one developed by Friedrichs (2010, pp. 7–8; see chapters ▶ "Investigations: Bank Fraud" and ▶ "Investigations: Money Laundering" in this encyclopedia).

Friedrichs' typology includes five categories based on criteria such as context, setting, agency, status or position of offender, primary victims, principal form of harm, and legal classification. **Corporate crime** as a type of white-collar crime, for example, refers to the "illegal and harmful acts committed by officers and employees of corporations to promote corporate (and personal) interests." Forms of corporate crime include corporate violence, corporate theft, corporate financial manipulation, and corporate political corruption or meddling. **Occupational crime** as a type of white-collar crime refers to the "illegal or harmful financially driven activity committed within the context of a legitimate, respectable occupation." Forms of occupational crime include retail crime, service crime, crimes of professionals, and employee crime. **Governmental crime** as a type of white-collar crime refers to "a cognate form of white-collar crime; a range of activities wherein government itself, government agencies, government office, or the aspiration to serve in a government office generates illegal or demonstrably harmful acts." Forms of governmental crime include state crime and political white-collar crime. Friedrichs' grouping of **"hybrid" crime** as a type of white-collar crime refers to **state-corporate crime**, **crimes of globalization**, and **high-finance crime**. Hybrid white-collar crimes involve some combination of governmental, corporate, international financial institution, or occupational crime. High-finance crime, for example, refers to "criminal activity in the realm of high-level finance, from banking to securities markets." **Enterprise crime**, **contrepreneurial crime**, **technocrime**, and **avocational crime** refer to what Friedrichs calls **"residual"** type of white-collar crime. Enterprise crime is characterized by the involvement of cooperative enterprises with syndicated (organized) crime and legitimate businesses. Contrepreneurial crime refers to swindles, scams and frauds that are made to look like legitimate businesses. Technocrime refers to the bundling of computers and other high technology with white-collar crime. Avocational crime refers to "illegal but non-conventional criminal acts committed by white collar workers outside a specifically organizational or occupational context, including income tax evasion, insurance fraud, loan/credit fraud, customs evasion, and the purchase of stolen goods."

Consequences and Impact

The 2010 National Public Survey on White Collar Crime shows that "white collar crime significantly affects U.S. citizens" (Huff et al. 2010, p. 22). The impact of white-collar crime can be indiscriminate and widespread, an effect that Moor and Mills (Moore and Mills 1990, p. 410) describe as "democratic." The consequences and impact of white-collar crime, therefore, have the potential to affect society at large, individuals, institutions, and the environment (Bruce and Becker 2007; Katz 2012). Such consequences may be physical, economic, political, societal, and psychological, and they may be long-lasting, large, or small, depending on the situation (Price and Norris 2009; Sutherland 1940, 1945; Shover et al. 1994; Moore and Mills 1990).

The consequences of white-collar crime usually are monetary and/or materialistic. Even in the early twentieth century, one white-collar criminal's financial harm over a year's time could be "six times as much as the annual losses from five hundred burglaries and robberies" of the same stores (Sutherland 1940, p. 5). Consequently, the harm caused by white-collar criminals has the potential to be much greater than the harm caused by conventional criminals (Sutherland 1940, 1945; Huff et al. 2010; Friedrichs 2010). The Association of Certified Fraud Examiners reports that the estimated cost of occupational fraud in 2017 was $4 trillion (ACFE 2018).

The actions of white-collar criminals have a negative effect on people's lives, often leading to "an astronomical toll in deaths, physical health, emotional suffering, and fiscal costs, one that dwarfs comparable losses to street crime" (Shover and Wright 2001, p. 49). For example, the opioid addiction epidemic in USA is claimed to be a result of drug companies' pushing sales and encouraging doctors to prescribe them in spite of the addictive nature of the drugs (Hadland et al.

2019). *The Center for Disease Control and Prevention* (CDC 2019) reports that more than 70,000 people died in 2017 from drug overdoses and about 68 percent of them were involved a prescription or illicit opioid. In an example from the food industry would be that consumers could be "killed by food poisoning, injured by unsafe products, defrauded by unscrupulous sales persons and are daily deceived by descriptions of goods and services" (Croall 2009, p. 130) without knowing that they had been victims of or harmed by white-collar crime.

Because white-collar criminals are highly trusted individuals, a violation of that trust affects social and political institutions. For example, damage to social relationships may lead to social disorganization on a large scale, resulting in a level of societal harm that is far greater than the dollar value of the financial harm (Sutherland 1940). Broken bonds of trust also can lead to the loss of "faith in and support for political institutions, public officials, and governmental processes. Citizens, for the most part, expect public officials to be honest themselves and also to deal unflinchingly with those who employ deceit and exploitation to prey on the public" (Moore and Mills 1990, p. 414). Whether the negative impact of white-collar crime is greater than negative impact of street crime is not known, primarily because white-collar crime is less visible to most people and awareness of such crimes is lower compared with street crime (Friedrichs 2010).

Conclusion

Scholars and practitioners disagree on the definition of the terms *white-collar criminal* and *white-collar crime*, though all can be said to have valid arguments for their views. Friedrichs (1992, p. 16) likens both terms to "a Chinese puzzle." He noted that "whichever way one turns with it new difficulties and conundrums are encountered" and suggests that having a comprehensive definition for both terms might be better than a single standard meaning for both terms (Friedrichs 1992). Without a consensus, debate over the definition of *white-collar criminal* and *white-collar crime* will continue.

White-collar criminals and the offenses they commit should be taken seriously for three reasons. First, white-collar criminals can be difficult to identify from outward appearances. As employees or owners of legitimate businesses or organizations, they work to garner the trust of colleagues and members of the community and then use that bond to conceal their involvement in illegal activity and deflect any suspicion of their involvement in such activity. Second, the consequences of white-collar crimes can be quite serious and widespread. The actions of even one white-collar criminal can affect and harm many people at the same time. The harm can spread from there to social and political institutions and to the environment. Third, the exploitation of technology by white-collar criminals may enable these individuals commit crimes that are not only broader in scope but also much easier to carry out even in younger ages (Payne 2018) than the age groups discussed in this chapter.

Cross-References

- ▶ Criminals: Blue-Collar Crimes
- ▶ Criminals: Motives
- ▶ Investigations: Bank Fraud
- ▶ Investigations: Criminal
- ▶ Investigations: Employee Theft of Employer Property
- ▶ Investigations: Fraud
- ▶ Investigations: Money Laundering
- ▶ Retail Security: Employee Theft

References

Association of Certified Fraud Examiners/ACFE. (2018). *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*. Retrieved on May 4 2019 from https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

Benson, M. L. (1985). Denying the guilty mind accounting for involvement in a white collar crime. *Criminology, 23*, 583–607.

Benson, M., & Gottschalk, P. (2015). Gender and white-collar crime in Norway: An empirical study of

media reports. *International Journal of Law, Crime and Justice, 43*(4), 535–552.
Benson, M. L., & Simpson, S. S. (2009). *White-collar crime: An opportunity perspective, criminology and justice series*. New York: Routledge.
Blickle, G., Schlegel, A., Fassbender, P., & Klein, U. (2006). Some personality correlates of business white-collar crime. *Applied Psychology, 55*(2), 220–233.
Bruce, A. S., & Becker, P. J. (2007). State-corporate crime and the Paducah gaseous diffusion plant. *Western Criminology Review, 8*(2), 29–43.
Bucy, P. H., Formby, E., Raspanti, M. S., & Rooney, K. E. (2008). Why do they do it? – The motives, mores and character of white-collar criminals. *St. Johns Law Review, 82*, 401–457.
CDC [The Center for Disease Control and Prevention]. (2019). *Opioid overdose: Understanding the epidemic*. Retrieved on August 14, 2019 from https://www.cdc.gov/drugoverdose/epidemic/index.html
Cohen, S., Blades, E., & Tacopino, J. (March 27, 2017). Investor burned by Madoff leaps to death from luxury hotel balcony. *New York Post* https://nypost.com/2017/03/27/man-leaps-to-death-from-sofitel-hotel/
Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology, 93*(2), 406–439.
Cressey, D. (1953). *Other people's money: The social psychology of embezzlement*. New York: Free.
Croall, H. (2009). White collar crime, consumers and victimization. *Crime, Law & Social Change, 51*(1), 127–146.
Cullen, F., Hartman, J., & Jonson, C. (2009). Bad guys: Why the public supports punishing white-collar offenders. *Crime, Law & Social Change, 51*(1), 31–44.
Daly, K. (1989). Gender and varieties of white-collar crime. *Criminology, 27*, 769–793.
Dhami, M. (2007). White-collar prisoners' perceptions of audience reaction. *Deviant Behavior, 28*, 57–77.
FBI. (2019). *White-collar crime*. Retrieved on May 5, 2019 from https://www.fbi.gov/investigate/white-collar-crime
Fishman, S. (Feb. 25, 2011), *The Madoff Tapes,* N.Y. MAGAZINE http://nymag.com/news/features/berniemadoff-2011-3/
Friedrichs, D. O. (1992). White collar crime and the definitional quagmire: A provisional solution. *The Journal of Human Justice, 3*(2), 5–21.
Friedrichs, D. O. (2010). *Trusted criminals: White collar crime in contemporary society* (4th ed.). Belmont: Wadsworth.
Geis, G. (1972). Criminal penalties for corporate criminals. *Criminal Law Bulletin, 8*, 377–392.
Gottschalk, P. (2014). Characteristics of rich white-collar criminals: An empirical study of a national sample. *International Journal of Ethics, 10*(3), 229–238.
Hadland, S. E., Rivera-Aguirre, A., Marshall, B. D. L., & Cerdá, M. (2019). Association of pharmaceutical industry marketing of opioid products with mortality from opioid-related overdoses. *JAMA Network Open, 2*(1), e186007. Retrieved on August 15, 2019 from https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2720914.
Huff, R., Desilets, C., & Kane, J. (2010). *The 2010 national public survey on white collar crime*. Fairmont: National White Collar Crime Center. Retrieved from https://www.nw3c.org/docs/research/2010-national-public-survey-on-white-collar-crime.pdf?sfvrsn=e51bbb5d_8.
Katz, R. (2012). Environmental pollution: Corporate crime and cancer mortality. *Contemporary Justice Review, 15*(1), 97–125.
Memmott, M. (October 27, 2011). 'Horrific' Situation Led Bernard And Ruth Madoff To Try Suicide, She Says. *NPR: The Two Way.* Retrieved from https://www.npr.org/sections/thetwo-way/2011/10/27/141749628/horrific-situation-led-bernard-and-ruth-madoff-to-try-suicide-she-says
Menard, S., Morris, R. G., Gerber, J., & Covey, H. C. (2011). Distribution and correlates of self-reported crimes of trust. *Deviant Behavior, 32*(10), 877–917.
Moore, E., & Mills, M. (1990). The neglected victims and unexamined costs of white-collar crime. *Crime and Delinquency, 36*(3), 408–418.
Paternoster, R., & Simpson, S. S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review, 30*, 549–583.
Payne, B. K. (2018). White-collar cybercrime: White-collar crime, cybercrime, or both? *Criminology, Criminal Justice, Law & Society, 19*(3), 16–32.
Perri, F. S. (2016). Red-collar crime. *International Journal of Psychological Studies, 8*(1), 61–84.
Piquero, N. L., Exum, M. L., & Simpson, S. (2005). Integrating the desire for control and rational choice in a corporate crime context. *Justice Quarterly, 22*, 252–280.
Piquero, N. L., Schoepfer, A., & Langton, L. (2008). Completely out of control or the desire to be in complete control? How low self-control and the desire for control relate to corporate offending. *Crime & Delinquency, 56*(4), 627–647.
Price, M., & Norris, D. M. (2009). White collar crime: Corporate and securities and commodities fraud. *The Journal of the American Academy of Psychiatry and the Law, 37*(4), 538–544.
Ragatz, L. L., Fremouw, W., & Baker, E. (2012). The psychological profile of white-collar offenders: Demographics, criminal thinking, psychopathic traits, and psychopathology. *Criminal Justice and Behavior, 39*(7), 978–997.
Saxby, P., & Anil, R. (2012). Financial loss and suicide. *The Malaysian Journal of Medical Sciences, 19*(2), 74–76.
Schoepfer, A., & Piquero, N. (2006). Exploring white-collar crime and the American dream: A partial test of institutional anomie theory. *Journal of Criminal Justice, 34*(3), 227–235.
Shapiro, S. P. (1990). Collaring the crime, not the criminal: Reconsidering the concept of white collar crime. *American Sociological Review, 55*, 346–365.
Shover, N., & Wright, J. (2001). *Crimes of privilege*. New York: Oxford University Press.
Shover, N., Fox, G. L., & Mills, M. (1994). Long-term consequences of victimization by white-collar crime. *Justice Quarterly, 11*(1), 75–98.

Sutherland, E. H. (1940). White-collar criminality. *American Sociological Review, 5*, 1–12.
Sutherland, E. H. (1945). Is "White collar crime" crime? *American Sociological Review, 10*(2), 132–139.
Sykes, G., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.
Wheeler, S., Weisburd, D. L., Waring, E., & Bode, N. (1988). White collar crimes and criminals (July 18, 2015). *American Criminal Law Review, 25*, 331–357.

Further Reading

Brickey, K. F., & Taub, J. (2017). *Corporate and white collar crime: Cases and materials*. New York: Wolters Kluwer.
Cengiz, M., & Roth, M. P. (2019). *The illicit economy in Turkey: How criminals, terrorists, and the Syrian conflict fuel underground markets*. Lanham: Lexington Books.
Edelhertz, H., & National Institute of Law Enforcement and Criminal Justice. (1970). *The nature, impact, and prosecution of white-collar crime*. Washington, DC: National Institute of Law Enforcement and Criminal Justice.
Kauzlarich, D., & Rothe, D. L. (2014). Crimes of the powerful. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 778–786). New York: Springer.
Pontell, H. N., & Rosoff, S. M. (2009). White-collar delinquency. *Crime Law Social Change, 51*(1), 147–167.
Wheeler, S. (1992). The problem of white-collar motivation. In K. Schlegel & D. Weisburd (Eds.), *White-collar crime reconsidered* (pp. 108–123). Boston: Northeastern University Press.

Critical Infrastructure: Commercial Facilities Sector

Ronald L. Martin
Capital Technology University, Laurel, MD, USA

Keywords

Cybersecurity Framework; Information security; Small business; CFS; CIP; Risk · RMF · SAFETY Act · PSA · NIPP · PPD-21 · Protective Security Advisors (PSA) · Project Responder 5 · EO 13636 · NCCoE · Cyber Community Voluntary Program C^3 · C^3VP · PR5

Definition

The Commercial Facilities Sector (CFS), one of the 16 critical infrastructure sectors, focuses on predominantly privately owned "sites that draw large crowds of people for shopping, business, entertainment, or lodging," including motion studios, malls, sports arenas, mixed-use facilities, and hotels (Cybersecurity & Infrastructure Security Agency/CISA n.d.).

Introduction

In 2013 the administration of the United States (US; The White House Office of the Press Secretary 2013) released Executive Order (EO) 13636, entitled Improving Critical Infrastructure Cybersecurity (Department of Homeland Security 2013). This EO directed (in part) the executive branch of government to strengthen cybersecurity practices and share cyber threat information (DHS 2013). Additionally, in the same year, the President Obama Administration released the US Presidential Policy Directive 21 (PPD-21). An essential action from the PPD was to require "The U. S. Department of Homeland Security (DHS) to revise the then 2009 National Infrastructure Protection Plan (NIPP) in 240 days from the release date of EO 13636" (DHS, 2013, para 10). The current NIPP issued in 2013 identifies 16 sectors aligned with PPD-21. "The 16 sectors are Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare, and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems" (CISA 2013, p. 9).

Another critical aspect of EO 13636 is it mandated the development of a cybersecurity framework and for the DHS to establish a voluntary critical infrastructure cybersecurity program. The Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 white paper was released by the National Institute of Standards and Technology (NIST) (NIST, 2014). Unlike other

NIST publications, the FICI white paper focused on the nonfederal government community to manage their cyber risks (NIST 2014). Within the 240 days from the release of EO 13636, the DHS established the Critical Infrastructure Cyber Community C^3 (pronounced "C Cubed") Voluntary Program (C^3VP). "The DHS C^3 VP provides cybersecurity resources to owners and operators of critical infrastructure; small and mid-size businesses; and State, Local, Tribal, and Territorial (SLTT) Governments. Per Executive Order 13636, the C^3 promotes the Cybersecurity Framework, which was developed by the National Institute of Standards and Technology (NIST)" (DHS 2013, p. 4). This program leverages the NIST Cybersecurity Framework, the expertise from academia and business along with state, local, tribal, and territorial (SLTT) government entities (C^3VP).

This entry addresses the Commercial Facilities Sector Plan (CFSP) (CISA 2015b). According to the DHS Critical Infrastructure Resource Center (CIRC), "The Retail Subsector alone generated more than $4.4 trillion in annual sales in 2008" (CIRC n.d., quick Facts). According to the CIRC this sector is divided into eight subsectors. "They are Entertainment and Media, Gaming, Lodging, Outdoor Events, Public Assembly, Real Estate, Retail, and Sports Leagues" (CISA 2015b, p. 3).

The NIST Computer Security Resource Center (CSRC) since the release of EO 13636 has led the cybersecurity doctrine for the CFS. In addition to the issuance of the FICI of 2014, the CSRC and the NIST Computer Science Division (CSD) established the National Cybersecurity Center of Excellence (NCCoE) in 2012 by the NIST in partnership with the State of Maryland and Montgomery County, Md. Although it was created before the release of EO 13636, the NCCoE was and is instrumental in providing cybersecurity doctrinal guidance to the commercial community.

Before the events of the Murrah Building Bombing; the terrorist attack on September 11, 2001; and the circumstances surrounding the response to Hurricane Katrina, there was little doctrinal guidance that identified the needs of the first responder community. Project Responder 5 (PR5) is the fifth iteration in the Project Responder series of studies to articulate the needs of the first responder community (PR5 2017). The initial effort was to "...improve the capabilities of local, state, and federal emergency responders..." (PR3 2014, P 49). Therefore, whether it is physical or cyber, the protection of and the response to Commercial Facilities Sector owners and operators are essential.

The Commercial Facilities Sector Subsectors

In 2015 the Commercial Facilities Sector Plan (CFSP) was released (CISA 2015b). The CFSP outlines eight subsectors that comprise this sector. This sector is overwhelmingly owned and operated by the private sector. As such, these operators must assess and mitigate vulnerabilities to their facilities. The cost to reduce vulnerabilities and to protect them is a funding challenge, particularly as the government has limited decision options as most of these are privately owned and operated. Table 1 shows the eight subsectors of the CFS based on information from CISA (2015b, p. 3). CFS is an important sector to the health and well-being of our way of life and serves as an economic engine for our nation. The CFS and its subsectors rely heavily on other critical infrastructure protection (CIP) sectors. The most critical are emergency services, financial services, energy, communications, healthcare, transportation services, government facilities, food and agriculture, information technology, and water and wastewater treatment sectors (CISA 2015b).

Executive Order (EO) 13636

In Executive Order 13636, titled Improving Critical Infrastructure Cybersecurity (Department of Homeland Security 2013a), the US policy is "to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy,

Critical Infrastructure: Commercial Facilities Sector, Table 1 Eight subsectors of the Commercial Facilities Sector

1. The *entertainment and media subsector* has approximately 49,000 establishments and represents over $1 trillion of media spend annually.
2. The *gaming subsector* consists of approximately 1,300 casinos and resorts. This subsector contributes over $35 billion in tax revenue.
3. The *lodging subsector* has over 52,500 hotel-/motel-based properties. These facilities generate over $150 billion in annual sales.
4. The *outdoor event subsector* represents over 550 amusement and theme parks. These facilities have approximately 290 million visitors annually.
5. The *retail subsector* has over one million buildings characterized as malls, shopping centers, and retail facilities. This subsector contributes over $2.5 trillion to the US Gross Domestic Product (GDP) annually.
6. The *real estate subsector* consists of over 1 million office buildings, 5.5 million multifamily rentals, and over 48 thousand self-storage facilities. This subsector contributes over $205 billion to the US GDP annually.
7. The *public assembly subsector* has over 124, 500 establishments characterized as stadiums, arenas, theaters, and cultural properties. These facilities in some cases share responsibilities with the sports league subsector. This subsector activity is a National Special Security Event (NSSE). An NSSE is an event that DHS has considered as critical in that it would be susceptible to a terrorist attack or criminal activity. NSSE has national and international significance. Events such as the US Presidential Democrat and Republican national conventions held in public assembly sector arenas qualify as an NSSE. The United States Secret Service releases an Annual Report. The latest report is the Office of Protective Operations 2017 Annual eport (CMR 2017). The United States Secret Service is the lead agency in charge of the planning, coordination, and implementation of security operations for the event (CMR 2017).
8. The *sports league subsector* like the public assembly subsector has one NSSE event. Each year the National Football Leagues "Super Bowl" is designated as an NSSE event. The NSSE designation aside, the subsector sports industry contributes over $480 billion annually.

and civil liberties" (EO 13636, Sect. 4 (a)). In enacting this policy, the EO required NIST to develop a voluntary risk-based Cybersecurity Framework. The resulting framework is a "…set of industry standards and best practices to help organizations manage cybersecurity risks…" (NIST Cybersecurity Framework 2014 p. 1). The resulting cybersecurity framework was created through a collaboration between NIST and the private sector and uses a common language to address and cost-effectively manage cybersecurity risk based on business needs without placing additional regulatory requirements on businesses.

National Infrastructure Protection Plan

The evolution of the US National Infrastructure Protection Plan (NIPP) sector program was documented by John D. Moteff, a specialist in the science and technology policy office of the Congressional Research Service (CRS). The first NIPP identified 17 sectors aligned with Homeland Security Presidential Directive 7 (HSPD-7). The next NIPP identified 18 sectors also aligned with HSPD-7 (CISA 2013). The EO 13636, titled Improving Critical Infrastructure Cybersecurity, issued and directed (in part) the executive branch of government to strengthen cybersecurity practices and share cyber threat information. The US Presidential Policy Directive 21 (PPD-21) established the 16 critical infrastructure sectors and aligned them with a federal government agency. These agencies are referred to as sector-specific agencies, (SSA), (CRS R42683) and (CRS RL30153).

The importance of the NIPP to all of the CIP sectors is it provides a framework for each sector to develop their visions, mission, and goals. In 2009, the framework had an element or chevron titled "Prioritize". Note the NIPP refers to each step of the risk management framework as chevrons (CISA 2013, Sect. 5, p. 15). Through the use of a critical infrastructure risk management framework, the NIPP lays out a protocol that establishes an information sharing environment (CISA 2013). A significant contribution is the establishment of a critical infrastructure risk management framework. The framework was amended in 2013, resulting in the removal of this chevron (CISA

Critical Infrastructure: Commercial Facilities Sector, Table 2 CFS goals and priorities of CFSP (CFSP 2015, Executive Summary, p. vi)

	Goals	Priorities
1	Strengthen trusted and protected sharing of information	"A" to improve information sharing; "B" the value of sector partnerships
2	Support the sector's needs for open access, public confidence, and economic vitality	"C" to expand training and exercises "D" to improve cybersecurity awareness
3	Increase capabilities and maintain advanced planning	"E" to enhance coordination
4	Assess and analyze threats, vulnerabilities, and consequences using the equation commonly referred to by NIST is risk = threat x vulnerability x consequence (Rochford Security Update 2017)	"F" to continue cyber and physical risk assessments
5	Promote continuous learning	"G" to facilitate information sharing of best practices for risk mitigation activities

2013, Sect. 5, p. 15). The 2013 NIPP recognized that each sector would have different priorities. As in the 2009 version of the NIPP, each chevron was required to address the three elements of the framework – physical, cyber, and human (CISA 2013, Sect 5, p. 15). These elements according to the NIPP should be integrated within each chevron, as appropriate.

A summary of the five chevrons indicates the general guidance the NIPP provides to the sectors. The first chevron is to set goals and objectives. This chevron requires the identification of specific critical infrastructure that is at risk (CISA 2013, Sect. 5, p. 16). Table 2 shows the CFS outline of the five goals of the CFS SSP (CISA 2015b) and their priorities. Finally, the sector mapped out 25 sector activities that align with and map to the goals and their corresponding priority.

The second chevron is to identify infrastructure. Here the sectors must identify assets, systems, networks, and sector interdependencies (CISA 2013, Sect. 5, pp. 16–17). DHS (2013c) assists the sector through the Protective Security Advisor (PSA) Program by providing "a robust operational field capability, with Regional Directors (RDs) and PSAs serving in 73 districts in 50 States and Puerto Rico" (DHS PSA Fact Sheet 2014).

The RDs and PSAs serve as the link to the Department of Homeland Security (DHS) infrastructure protection resources. The PSAs have five mission areas that directly support the protection of critical infrastructure:

- Plan, coordinate, and conduct security surveys and assessments – PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.
- Plan and conduct outreach activities – PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of IP priorities.
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events – PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.
- Respond to incidents – PSAs plan for and, when directed, deploy to Unified Area Command Groups, Joint Operations Centers, Federal Emergency Management Agency Regional Response Coordination Centers, and/or State and local Emergency Operations Centers in response to natural or man-made incidents.
- Coordinate and support improvised explosive device awareness and risk mitigation training. (DHS 2014, PSA Fact sheet, page 1).

They assist with and support National Special Security Events (NSSEs) and respond to incidents. Finally, they coordinate and support improvised explosive device awareness and risk mitigation training (CISA Protective Security Advisor Program).

The third chevron is to assess and analyze risks. Risks are characterized as threats, vulnerabilities, and consequences. The organization owning or operating the infrastructure should develop risk scenarios where events could be assessed in terms of their threat, vulnerabilities, and impacts to the continuity of the enterprise (CISA 2013, Sect. 5, pp. 17–18). As previously mentioned, the DHS PSA Program may assist the sector. The PSAs can come at no cost to the stakeholder. The advisor will use the computer-based assessment tool or CBAT and the infrastructure survey tool or IST to provide the stakeholder with a detailed assessment report (CFS SSP 2015b, Sect. 3.1, pp. 21–22).

The fourth chevron requires the company to implement risk management activities. The stakeholder exercises the process to identify, deter, detect, disrupt, and prepare for threats and hazards. The infrastructure managers attempt to reduce their vulnerabilities and minimize their exposure to adverse consequences. NIPP recommends that critical infrastructure stakeholders prepare their infrastructure to become resilient. This circumstance means that there must be a responsible response to events along with the ability to recover (CISA 2013, Sect. 5, pp. 18–20). In response, the CFSP provides that stakeholders participate in various information sharing activities. The subsector participants establish security alliance councils to engage in cross-sector and subsector principals.

Two essential programs will assist the sector with this information sharing program. The first is the InfraGard program. "InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure" (retrieved from InfraGard homepage on May 5, 2019, para 1). The second initiative is the DHS SAFETY Act Program. "As part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) of 2002" (DHS S&T 2016, para 1). The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management. The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing and commercializing technologies that could save lives (DHS S&T 2016, para 2). The CFSP has a priority for members of the sector to participate in this program and use technologies that are SAFETY Act designated or certified (CFS SSP 2015b, Sect. 3.1, pp. 21–22).

The fifth NIPP risk management framework chevron is measuring effectiveness. The NIPP requires sector stakeholders to evaluate achievement of goals, learn, and adapt during and after exercises and incidents (CISA 2013, Sect. 5, p. 20). To measure the effectiveness of the CFS activities, the CFSP outlined 25 activities with expected metrics. As mentioned earlier in this article, each CFS activity has one or more priority designations (CFS SSP 2015b Sect. 4.1, pp. 28–29) Also the CFSP Appendix B provides a chart that depicts alignment with the NIPP 2013 call-to-action imperatives. Appendix C outlines Sector-Specific Tabletop Exercise Programs (SSTEP) and Independent Study courses, publications, and tools such as the cybersecurity evaluation program and cyber resilience review. For those stakeholders involved with industrial control systems (ISC), the ICS Cyber Emergency Response Team (ISC-CERT) makes available the cybersecurity evaluation tool (CSET) (CFS SSP 2015b Appendices B and C, pp. 36–44).

National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST), as a partner with the Small Business Administration and the Federal Bureau of Investigation in an information security awareness outreach to the small business community, provides publications and information to assist

commercial enterprises with their cybersecurity initiatives. Many commercial enterprises do not place a high priority on cybersecurity. The security of client and customer information, systems, and networks takes a backseat to the operation of the business. However, their customers, employees, and trading partners' cybersecurity and the protection of their personal information are imperative.

To better address these risks, NIST publishes documents to inform and educate the business community on cybersecurity policies and best practices. Additionally, NIST established the National Cybersecurity Center of Excellence (NCCoE). The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md. NCCoE is a collaborative hub where industry organizations, government, and academic institutions collaborate. This collaboration addresses cybersecurity issues. This program is an important public-private partnership. NCCoE enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. For example, the NCCoE Consumer and Retail Sector is one area of the center's key initiatives. The work of this initiative concentrated on consumer-facing businesses cybersecurity posture. Other programs or use cases are financial services sector, health information technology sector, hospitality sector, manufacturing sector, energy sector, transportation sector, public safety, and first responder sector. These projects of the NCCoE are aligned closely with the critical infrastructure sectors. The key emphasis is to enhance the cybersecurity posture of the CFS (NCCoE 2012).

Critical Infrastructure Cyber Community Voluntary Program C^3

EO 13636 required NIST to develop and publish a voluntary risk-based Cybersecurity Framework. The EO also required DHS to develop cybersecurity information to small and midsize businesses. Thus, the Critical Infrastructure Cyber Community Voluntary Program C^3 (C^3VP) was released on February 12, 2014 (DHS 2014). This program supports the NIST Cybersecurity Framework. The key initiative of this program is the Cyber Resilience Review (CRR). This resilience review is a process improvement model where stakeholders could self-assess their organization's current state of cybersecurity preparedness. The Cyber Resilience Review evaluates capabilities across ten domains. These domains are "asset management, control management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependency management, situational awareness training and awareness" (CRR 2014). The CFS SSP recommends the use of the Cyber Resilience Review as a tool for managing cyber risks (CFS SSP 2015b, Sect. 3.2, pp. 23–24). It is important that a cross-functional team within an organization participate with this review. Members from the chief security office, information technology, operations, and disaster recovery organizational elements participate. This list is not all-inclusive. Organizations may opt to include human resources, financial management, and facility management (CRR 2014). The Cyber Resilience Review is an inclusive process versus an exclusive program. This process invites all stakeholders to provide input to the review's analytical process.

Critical Infrastructure Response

A key component of business sustainability, continuity, and recovery is the emergency response environment. The DHS Science and Technology Directorate has funded and supported Project Responder 5 (PR5 2007). The PR5 report is a report of the examination of the response based on the current threat environment, the responder capabilities, and the application of available technological resources.

Therefore, the PR5 report provides a substantial nexus to the CFS. Homeland Security Presidential Directive 8 defines a first responder as "The term 'first responder' refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002" (6 U.S.C. § 101), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations" (HSPD-8 2003 para 2 (d)).

The PR5 report describes 37 capabilities of needs encountered by first responders grouped into 9 areas. These include "1. risk assessment and planning, 2. communication and information sharing, 3. command, control and coordination, 4. situational awareness, 5. training and exercise, 6. casualty management, 7. Responder health and safety, 8. Intelligence and investigation, and 9. Logistics and resource management" (PR5 2017 Fig. 8. PR5 capability needs p. 25). The response to incidents incurred by stakeholders of the CFS is critical to the survivability of sector organizations. Therefore, there is an increased need for the CFS to establish an active information sharing program with first responders.

Conclusion

Before the promulgation of the CIP program and the release of the CFS SSP, the preponderance of commercial sector protection initiated was a state and local responsibility. The diversity of the CFS and myriad of threats presented a unique challenge to the stakeholders of the sector. To rise to the challenges, the CFS provides an actual government and private sector collaboration. In the CFS SSP, the commercial enterprises have the governance to develop plans and programs to protect their resources. The openness of sector facilities presents serious vulnerabilities. This unencumbered access to the sector facilities present challenges to the first responder community. EO 13636 required DHS and NIST to issue governance. NIST published the Framework for Improving Critical Infrastructure Cybersecurity. DHS established the Critical Infrastructure Cyber Community Voluntary Program C^3 to enhance the CFS stakeholder's ability to evaluate their resilience posture. The Cyber Resilience Review is a process improvement model where stakeholders could self-assess their organization's current state of preparedness.

Additionally, DHS, through the release of Project Responder 5 report, identified 37 capabilities of first responder needs, grouped into 9 areas. This effort provided a substantial nexus between the federal government, the stakeholders of the CFS, and the first responders tasked with the responsibility to protect the nation. With the continuing threat to the sector's cyber infrastructure, NIST has partnered with the Small Business Administration and the Federal Bureau of Investigation to publish the NIST Interagency Report titled Small Business Information Security: The Fundamentals. These reports, as well as the collaboration between government and private industry through the InfraGard program, will provide a vital conduit to mitigate future challenges.

Cross-References

- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Emergency Services Sector
- ▶ Critical Infrastructure: Government Facilities Sector (GFS)
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector

References

Bush, G., & Office of the Press Secretary. (2003). *Homeland Security Presidential Directive/HSPD-8- National Preparedness*. Washington, DC: Executive Office of the President of the United States. https://fas.org/irp/offdocs/nspd/hspd-8.html.

Critical Infrastructure Resource Center (CIRC). (n.d.). *Understanding the commercial facilities sector*. Washington, DC: U. S Department of Homeland Security. June 18, 2019 http://www.humtech.com/fema/CI_RC/comFac1.htm

CISA (2013). National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2014a). *Critical infrastructure cyber community C3 voluntary program*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/ccubedvp.

Cybersecurity and Infrastructure Security Agency (CISA). (2014b). *Stakeholder engagement and critical infrastructure resilience cyber resilience review, (CRR)*. Washington, DC: U.S. Department of Homeland Security. http://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). (2015a). Commercial facilities sector. Washington, DC: Department of Homeland Security. https://www.dhs.gov/cisa/commercial-facilities-sector

Cybersecurity and Infrastructure Security Agency (CISA). (2015b). *Commercial facilities sector-specific plan: An annex to the NIPP 2013*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-commercial-facilities-2015-508.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). Protective security advisors program. https://www.dhs.gov/cisa/protective-security-advisors

Cybersecurity & Infrastructure Security Agency/CISA (n.d.). Protective security advisors. https://www.cisa.gov/protective-security-advisors

Department of Homeland Security. (2009). *National Infrastructure Protection Plan (NIPP) partnering to enhance protection and resiliency*. Washington, DC: U. S Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Department of Homeland Security (2013). Improving critical infrastructure cybersecurity. https://www.cisa.gov/sites/default/files/publications/19_1115_dhs-eo13636-analytic-report-cybersecurity-incentives-study%281%29.pdf.

Department of Homeland Security. (n.d.). Commercial facilities sector. https://www.dhs.gov/cisa/commercial-facilities-sector (6.11.2019).

Department of Homeland Security, Science and Technology Directorate. (2016). *Research and development partnerships – SAFETY act for liability protection fact sheet*. Washington, DC: U. S Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/Safety%20Act%20for%20Liability%20Protection_0.pdf.

Kristen, D. (2017). *Rochford-Security–update*. Gaithersburg: National Institute of Standards and Technology. https://www.nist.gov/sites/default/files/documents/2017/06/12/2._rochford_-_security_update.pdf.

Moteff, J. (2012). *Critical infrastructures: Background, policy, and implementation*, issues for Congress (CRS R42683). Washington, DC: Congressional Research Service. https://fas.org/sgp/crs/homesec/R42683.pdf

Moteff, J. (2015). *Critical infrastructures: Background, policy, and implementation* (CRS RL30153). Washington, DC: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/homesec/RL30153.pdf

National Cybersecurity Center of Excellence (NCCoE). (2012). NCCoE-Brochure. Gaithersburg: National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/library/nccoe-brochure.pdf

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity, (FICI), Version 1.0. Washington DC, US Department of Commerce. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity version 1.1*. Washington, DC: U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

National Protection and Programs Directorate. (2014). *Press release DHS launches the C3 voluntary program, a public-private partnership to strengthen critical infrastructure cybersecurity*. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/blog/2014/02/12/dhs-launches-c%C2%B3-voluntary-program.

National Protection and Programs Directorate's Office of Infrastructure Protection. (2014). *Fact sheet: Protective Security Advisor Program*. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/PSA-Program-Fact-Sheet-05-15-508.pdf.

Office of Cybersecurity & communications (2014). Cyber resilience review fact sheet. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/Cyber-Resilience-Review-Fact-Sheet-508.pdf

Office of Infrastructure Protection. (2006). National Infrastructure Protection Plan. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf

Office of Infrastructure Protection (IP) (2014). Cyber Community Voluntary Program C3 (C3VP) Web Site. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/ccubedvp

Office of Protective Operations. (2017). Annual report CMR-2017_Annual_Report_online, U. S. Secret Service, Washington, DC. https://www.secretservice.gov/data/press/reports/CMR-2017_Annual_Report_online.pdf

Office of the Private Sector. (2018). *Office of the private sector (OPS) fact sheet*. Washington, DC: Federal Bureau of Investigation. https://www.fbi.gov/file-repository/ops-factsheet-8-3-18.pdf/view.

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals* (NISTIR 7621 R-1). Gaithersburg: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

Science and Technology Directorate. (2016). *Research and development partnerships – SAFETY Act for liability protection*. Washington, DC: U. S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/Safety%20Act%20for%20Liability%20Protection_0.pdf.

Science and Technology Directorate. (2017). *Project responder five final reports*. Washington, DC: U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/Project-Responder-5-Report_170814-508.pdf.

The White House Office of the Press Secretary (2013). Presidential Policy Directive–Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Further Reading

Cybersecurity and Infrastructure Security Agency (CISA). (2019). *National critical functions an evolved lens for critical infrastructure security and resilience*. Washington, DC: U. S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). (2019). *National critical functions set*. Washington, DC: U. S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/national-critical-functions-set-508.pdf.

Cybersecurity and Infrastructure Security Agency (CISA). (2019). *National critical functions reducing national risk*. Washington, DC: U. S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/19_0430_cisa_nrmc-reducing-national-risk.pdf.

Critical Infrastructure: Critical Manufacturing Sector

Brian Keith Simpkins
Homeland Security Program, Eastern Kentucky University, Richmond, KY, USA

C

Keywords

Dependencies · Infrastructure concentration · Interdependencies · Risk · Supply chains

Definition

Critical Infrastructure	"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [USA PATRIOT] Act, 2001, § 1016).
Critical Manufacturing Sector	Privately owned and operated assets (manufacturing plants, logistical distribution facilities, storage facilities, and center business offices) that convert raw materials and manufactures specialized materials and equipment vital to the construction, electrical, defense, and industries among others (U.S. Department of Homeland Security [DHS] 2015a).

Introduction

The Critical Manufacturing Sector (CMS) is just one of many critical infrastructure sectors that play an important role in support of a democratic nation and help to ensure US economic vitality and national security. However, the CMS is not immune to challenges as supply chain disruptions at the national and global levels can induce severe consequences (Executive Office of the President 2017). These high-level challenges are just the beginning as the CMS faces a myriad of risks (natural hazards, technological hazards, and human-caused incidents) and cross-sector dependencies, which can result in significant cascading effects.

The remainder of this entry provides a general overview of the CMS to enable a general understanding. Within the discussion, key operational characteristics of the CMS are reviewed along with a description of the current threat and hazard picture to include critical cross-sector dependencies. This discussion will also include mission, goals, and priorities of the CMS along with the partnership structure. Partnerships and information sharing within the CMS are elevated due to a high private ownership share of sector assets. Overall, this entry provides a basic understanding of the CMS to enable critical evaluation of current policies, practices, and needed activities to address gaps in security and resilience.

Sector Overview

The CMS consists of the manufacturing industries which have significant national economic implications and are considered crucial for operations within other infrastructure sectors. The main activities of the CMS are to process and manufacture. Processing involves converting raw materials and primary metals into useable products that are subsequently utilized in manufacturing. Specific manufacturing that is deemed critical includes machinery (engine, turbines, power-transmission, heavy machinery), electrical components (motors, transformers, generators), and transportation (for surface, water, and rail modes). Further, the CMS produces highly specialized parts and equipment essential to specific US industries, particularly the Defense Industrial Base Sector. Additionally, the CMS produces the backbone materials and components for the Energy Sector and Transportation Systems Sector. Therefore, failures and/or disruptions in the CMS can cause severe consequences in terms of economic impact and cascading effects to other infrastructure sectors. Lastly, the US economic prosperity and continuity are dependent on the CMS, and this sector's production comprises 12 percent of the nation's gross domestic product (GDP) and employs approximately 12 million individuals.

Sector Components and Assets

Due to the diversity of manufacturers and high private ownership share, the CMS is organized into four subsectors based on functions and operations. Regardless of subsector, facilities (manufacturing, processing, and distribution), offices (sales and headquarters), and product storage are included as key assets. Characteristics of each subsector are provided below per the *Critical Manufacturing Sector-Specific Plan* (CM SSP).

Primary Metals Manufacturing: Converts raw materials into assemblies, intermediate products, and end products. These products can include sheet metal, bar stock, I-beams, slabs, or pipes. Processes aluminum, iron, and steel that supports transportation, urban centers, energy supply, clean water, safe food, and defense. There are 4,556 manufacturers in this subsector.

Machinery Manufacturing: Produces engines, turbines, and power-transmission equipment. Products support infrastructure and primary operations in a number of critical US industries. Includes heavy-equipment manufacturing. There are 24,124 manufacturers in this subsector.

Electrical Equipment, Appliance, and Component Manufacturing: Produces specialized equipment, assemblies, intermediate products, and end products for power generation.

These products include transformers, electric motors and generators, and industrial controls. There are 5,765 manufacturers in this subsector.

Transportation Manufacturing: Produces cars and trucks, aircraft and component parts, aerospace products and parts, railroad cars and other railroad products, and other transportation equipment. There are 11,814 manufacturers in this subsector. (DHS 2015a, p. 4).

Key Sector Operating Characteristics

The importance of the CMS can be summed in one specific figure: CMS produces 60% of all of US exports. Facilities, employees, suppliers, and customers around the world are part of the complex international, interdependent networks of raw materials and finished products in which CMS assets operate. Although it improves production agility, this complex global network increases the exposure of the CMS to a myriad of risks and conditions. In fact, disruptions in supply chains are one of the top security and resilience concerns of the CMS. This is because present supply chains focus on efficiency (e.g., lean inventories) and just-in-time practices, but this also increases vulnerability of CMS assets to long-term disruptions. This is because CMS assets are part of the network that links suppliers, vendors, partners, integrators, contractors, and customers not only to their asset, but also to other industries and businesses. Therefore, CMS assets must ensure resilience against supply chain disruptions, which includes constant monitoring and a proactive stance to mitigate any disruptions.

Sector-Specific Agency

The US government by itself cannot create a secure and resilient CMS, especially in relation to high private sector ownership. Rather, the end goal requires a dedicated whole-of-nation approach involving public and private stakeholders. Leading this whole-of-nation approach is the designated Sector-Specific Agency (SSA) as defined in *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience* (Executive Office of the President 2013). The designated SSA for the CMS is DHS. More specifically, the Office of Infrastructure Protection is the delegated responsible entity within DHS.

Sector Partnerships

The *National Infrastructure Protection Plan* (NIPP) defines a partnership structure for the infrastructure sectors that is facilitated through Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs). The SCCs are comprised of owners and operators and enable them to work directly with one another. Typically organized under subsectors within an overall infrastructure sector, SCCs are self-organized, self-run, and self-governed councils consisting of owners and operators and their representatives and serve as principal collaboration points between the GCCs and the SSAs. As for the GCCs, SSAs work closely with state, local, tribal, and territorial (SLTT) agencies through the GCCs to enable sharing of actionable, relevant risk information; exchanging of best practices; building of cross-sector situational awareness; and enabling risk-informed decision-making.

The importance of SLTT agencies is illustrated by the fact they work in close proximity to the owners or operators of the CMS. Coordination with SLTT agencies is imperative as all incidents start local and these agencies are first to respond to any incident. Therefore, SLTT agencies provide important local capability to include mutual aid agreements and communication plans where appropriate. It is the responsibility of the SSA to cultivate relationships and information sharing between SLTT agencies and the GCCs and SCCs to enhance situational awareness and addresses identified risks to the CMS. This illustrates that the success of a sector's partnership model depends on the ability to leverage knowledge, capabilities, and resources through GCC and SCC activities. Through this collaboration exchange, owners and operators of CMS assets can better understand risks and interdependencies

and develop appropriate security and resilience strategies to mitigate identified risks.

Sector Risks

Despite the diverse collection of assets within the CMS, common risks exist that each sector must address. Natural disasters, active shooters, and terrorist threats are persistent risks across the CMS as well as geopolitical events due to its linkage to a global supply chain (DHS 2014). Further, cyber attacks risks continue to grow as reliance on networked systems continues to rise. This illustrates the need to comprehensively examine risks across the CMS through existing partnership structures in an effort to ensure security and resilience. Although numerous risks can be discussed, the following sections focus on those risks deemed significant. It is acknowledged there are other significant risks to the CMS, but these risks will not be discussed for the sake of brevity. Expanded information on risks to the CMS is accessible via the CM SSP.

Concentration

Within the CMS, geographic concentration helps to reduce overall costs due to a localization of expertise and reduction in logistical operations. However, this concentration can increase vulnerability to geographic risks and local disasters that can produce cascading effects (Parfomak 2008). Although the CMS is widely dispersed across the nation, certain subsectors or aspects are concentrated in specific regions, which require additional security and resilience activities. For example, CMS facilities are geographically concentrated around coastal ports (Parfomak 2008). This placement supports the importing and exporting logistics of materials and products within the sector. Further, the global supply chain also converges in strategic geographic areas thereby creating chokepoints that can cause and magnify disruptions. This is especially relevant to global maritime transportation in areas such as the Malaccan Strait (Indian Ocean), Gulf of Hormuz (Middle East), and the Panama Canal (links Atlantic and Pacific Oceans). However, disruption in access to rare and and/or scarce raw materials may also create vulnerabilities. Therefore, global networks must be constantly monitored in order to anticipate, respond to, and mitigate possible disruptions.

Natural Hazards, Climate Change, and Extreme Weather

Natural hazards are a constant threat to all critical infrastructure sectors. Severe storms, hurricanes, earthquakes, tornadoes, volcanoes, drought, floods, landslides, tsunamis, and wildfires can cause significant property and economic damage, threaten safety of employees and facilities, and restrict access to critical resources such as power, water, transportation, and food supplies. Natural threats are typically present in defined geographic areas thereby increasing the vulnerability of physical assets and employees in those areas. Specific natural threats that can affect the CSM both domestically and globally should be identified according to likelihood of occurrence. Global weather is important as well in the CMS because natural disasters in other global regions can result in cascading disruptions in supply chains. This is in addition to natural disasters interrupting critical dependent sector services (e.g., Energy Sector) resulting in delays or shutdowns.

Today, the risk of natural hazards is increasing due to climate change. Although it occurs gradually over time, impacts from climate change are presently viewable and are projected to worsen in the future. In fact, the CMS is already impacted by climate change both in the United States and globally. This has led to both DHS and the US Department of Defense (DOD) to view climate change as a threat multiplier. Natural hazards and extreme weather result in risks such as power interruptions, wildfires, regional flooding, droughts, and severe storms, and each carries its own consequences to CMS assets. However, climate change has made extreme weather events more frequent and intense.

Therefore, climate change has altered the frequency and intensity of natural hazards and severe weather, which can produce significant cascading effects on the CMS. For example, the Energy Sector can be stressed through extreme heat and diminished precipitation thereby causing possible power interruptions to CMS assets. Further, sea-level rise accompanied by storm surge increases coastal flooding, which impacts CMS assets geographically concentrated in coastal areas. An example of this is the impact on shipbuilding operations in the Newport News and Norfolk (VA) area (Parfomak 2008). Therefore, actions related to risk assessment, mitigation, resilience, and adaptation must include climate change in addition to natural hazards and severe weather. If not, historical examples provide poignant examples of how the CMS has been affected significantly by climate-related hazards.

Active Shooter/Armed Attacker

The DHS Interagency Security Committee (ICS) defines an active shooter as "an individual or individuals actively engaged in killing or attempting to kill people in a populated area" (Interagency Security Committee 2015, p. 1). Although a firearm is the most common weapon used in active shooter/armed attacker events, other weapons – knives, bats, etc. – can be utilized to harm innocent individuals. Active shooter events pose significant challenges to all CMS assets (such as workplace violence) as the incidents do not follow a specific pattern or a method to the selection of victims. Therefore, active shooter incidents are sometimes impossible to predict and/or prevent. This is further complicated by the fact that active shooter incidents require less resources and planning than other attack methodologies, such as an explosive attack. The frequency of active shooter incidents has increased over the past several years, and incidents have occurred at numerous CMS assets.

As illustrated in previous events, active shooter incidents quickly evolve and are dynamic. Virtually all active shooter incidents end via force by responding law enforcement agencies or through suicide by the assailant. Therefore, CMS assets and on-site individuals must be prepared to address and mitigate an active shooter incident prior to arrival of law enforcement resources. This preparedness can be in the form of security protocols as well as ensuring employees are trained both mentally and physically to deal with an active shooter situation. Overall, recent events illustrate the need to reduce the risk of active shooter incidents to include ongoing preparedness and strengthening of prevention and protection efforts.

Cyber Attacks

Adversaries have successfully executed cyber attacks against the CMS over the past several years (Bennett 2016). These attacks have released unimaginable amounts of private and confidential data and have resulted in damages in excessive of hundreds of millions of dollars. Cyber attacks do not only come from sole individuals or groups but also from state-sponsored activities from countries such as Russia, China, and North Korea. This has led to an increase in hacktivism or politically motivated cyber attacks. Another area of concern related to cyber attacks is the increasing use of comprehensive, computerized building management systems, which control heating, ventilation, and air conditioning (HVAC) systems, access control systems, surveillance systems, etc. These systems reside on networks which makes them vulnerable to a cyber attack or a significant network outage. Of particular importance is the possibility of a cyber attack leading to local or system-wide outages resulting in the loss of ability to control physical access, lighting, temperature, or even life-safety systems.

The more significant danger of cyber attacks in the CMS is intrusion into industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Unauthorized intrusion into these systems has the potential to result in severe negative impacts to the

CMS asset that could cascade and create impacts in other sectors dependent on specific production provided by the CMS. As such, the cyber risk has been recognized by the CMS as a high-priority concern (DHS 2015b; Government Accountability Office 2015). In response to the cyber risk, CMS owners/operators can follow cybersecurity implementation framework guidance detailed in the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST 2015).

The recognition and focus on cyber attacks are important due to recent successful, high-profile cyber attacks in the CMS. In fact, the US Computer Emergency Response Team (2017) has reported that threat actors are increasingly targeting assets within the CMS through the use of "open-source reconnaissance, spear-phishing emails (from compromised legitimate accounts), watering-hole domains, host-based exploitation, and ongoing credential gathering" (p. 1). Further, the number of investigations into cyber attacks by DHS increases each year, in which most attacks are related to spear-phishing campaigns. The increasing reliance on computer networks for operations as well as security presents increased risk of cyber attacks by individual external (hacktivists) and internal (sabotage by former employees) to the CMS.

Terrorism and Violent Extremism

Certain characteristics of the CMS increase the target attractiveness to a potential terrorist or violent extremist. As such, the threats of attack from terrorists and violent extremists are major contributors to the risk profiles of the CMS. Overall, the CMS represents attractive targets to both domestic and international terrorist groups as well as violent extremists. Therefore, the CMS must be cognizant of the changing domestic and international terrorist threats, including the threat from homegrown violent extremists (HVEs). Some counterterrorism experts consider HVEs as the most immediate threat to US infrastructure. One of the reasons is that HVEs can be US citizens or legal permanent residents, which enables them to freely operate throughout US society. This increases the risk of insider threats in which radicalized individuals who work in the CMS can exploit vulnerabilities through their inside knowledge. However, HVEs typically have less access to resources and training, which results in their planning and attack methodology being simpler and less technical. This asymmetric threat presents challenges in predicting and interdicting attack plots.

Unmanned Aircraft Systems

Unmanned aircraft systems (UAS) are an emerging threat to the CMS. The increased use of UAS throughout the Nation is a serious concern due to the ability to use them to cause damage to persons and property (Coullahan 2017). UAS are particularly worrisome to CMS assets because they enable individuals to access restricted and previously unreachable areas, such as the air space above a facility. The ability to access this space could provide opportunities to cause significant damage or casualties. Further, adversaries can utilize UAS to obtain information about a facility – security layouts – thereby providing highly valuable information for planning and executing an attack.

Supply Chain Disruptions

As previously discussed, today's global supply chain is optimized for productivity and efficiency. Therefore, disruptions in the supply chain can quickly cause cascading effects especially if raw materials cannot reach CMS assets. An absence of raw materials will also cause the inability to manufacture and deliver finished products. Disruptions in the global supply chain are the result of one or many causes, including civil unrest and natural disasters. Technology also plays a role as the Maritime Transportation System (MTS) is dependent on Global

Positioning Systems (GPS) and resulting positioning, navigation, and timing data. Disruptions in the ability to obtain GPS data through either unintentional or intentional (cyber attack) means have the potential to create significant cascading supply chain disruptions. Therefore, CMS assets must be able to withstand infrequent, yet high-impact risks related to the global supply chain.

Global Political and Social Implications

One important aspect of the US supply chain is that CMS assets are now more dependent on raw materials and minerals from foreign countries due to declining mining activity in the United States. This is in addition to CMS assets utilizing foreign markets to reduce overall costs related to component manufacturing, equipment, machinery, and labor. This dependence on international networks increases risk for CMS assets to a host of global risks. In addition to the global supply chain, the CMS must now keep abreast of global attitudes toward the United States, geopolitical unrest, economic conditions, and other risk factors associated with global markets. These risk and variables impact foreign operations, global supply chain providers, and raw material access and can result in significant cascading disruptions.

Primary Sector Dependencies and Interdependencies

Today, the US critical infrastructure sectors are highly dependent and interdependent on one another through physical and cyber linkages. After a natural disaster, man-made incident, or technological accident, a significant failure in one sector – such as in the Energy Sector or Water and Wastewater Systems Sector – has the potential to cascade and create significant impacts to other regions. Currently, the CMS has interdependencies with the sectors of Communications and Information Technology, and dependencies on the sectors of Chemical, Energy, Financial, Transportation Systems, and Water and Wastewater (DHS 2014, 2015a). Descriptions of select dependencies and independencies are provided below.

Energy: Provides power, which supports CMS functions. This is the primary dependency for the CMS. Without power, CMS assets cannot not function for an extended period of time, as access to backup power is often limited in scope. An interruption to the power supply would directly impact all CMS assets located in the affected electrical service region and could have cascading effects on other sectors.

Water and Wastewater Systems: Provides a supply of potable water and handles the treatment of wastewater. In some cases, continuous water sources are essential for critical manufacturing processes. Without these services, CMS assets would be forced to be shut down until services are restored.

Transportation Systems: Transportation systems allow employees and customers to travel to and from CMS assets to receive products and supplies. Manufacturers depend on multiple modes of transportation (aviation, freight rail, highway, and maritime) for the secure movement of raw materials and finished products.

Financial Services: Provides financial services to enable CMS assets to conduct daily business operations.

Communications: CMS asset owners and operators rely on the Communications Sector for telecommunications access for operations and logistics.

Information Technology: Enables day-to-day operations and financial transactions. Underpins supply chain coordination and control system processes.

Chemical: A consistent supply of a range of chemicals is required in multiple CMS processes (DHS 2015a, p. 3, 6–7).

In addition to external dependencies and interdependencies between sectors, the CMS also experiences internal interdependencies similar to other infrastructure sectors. For example, CMS assets engaging in Machinery Manufacturing is dependent on products from Primary Metals Manufacturing assets.

However, Primary Metals Manufacturing assets are also dependent on Machinery Manufacturing assets to produce machinery and parts to enable raw material processing. Therefore, interdependency in this example is a two-way street relationship.

Today, the continual operation of the CMS is dependent and interdependent on other infrastructure sectors similar to those sectors that are interdependent with the CMS. Greater dependences and interdependencies, especially in the cyber realm related to communications and information technology, create the potential that even a localized disruption will have the ability to cascade to numerous CMS assets. This is in addition to the vulnerabilities within the global and national supply chains that can pose significant disruptions to the CMS.

Sector Mission, Goals, and Priorities

In alignment with the NIPP, each SSA develops a specific mission for their respective infrastructure sector, which is defined in individual SSPs. Listed below is the specific mission statement for the CMS.

Mission Statement: Strengthen the security and resilience of the Critical Manufacturing Sector by building an active public-private partnership to coordinate efforts that enable proactive risk reduction and effective response, recovery, and adaptation (DHS 2015a, p. 15).

In addition to defining the mission, the CM SSP identifies specific goals and priorities, which are aligned with the five overall national goals defined in the NIPP.

Sector Goals

1. Improve information sharing and promote continuous learning. *(NIPP Goal #4).*
2. Identify sector-specific risks. *(NIPP Goal #1).*
3. Develop cost-effective strategies to reduce risks. *(NIPP Goal #2).*
4. Support research and development efforts and advanced planning to ensure rapid response and recovery. *(NIPP Goals #3 and #5)* (DHS 2015a, p. 15).

Sector Priorities

1. Evaluating interdependencies with other sectors and within supply chains.
2. Increasing engagement and collaboration both within the sector and with other critical infrastructure sectors.
3. Raising risk awareness at executive levels.
4. Improving cybersecurity knowledge, tools, capabilities, and practices.
5. Participating in cross-sector trainings and exercises to improve response and recovery. (DHS 2015a, p. 15).

Conclusion

As with all US infrastructure sectors, the CMS is vitally important to individuals, communities, and the nation overall. Another important aspect of the CMS is that it helps preserve the American way of life. For example, the CMS not only supports employment but also manufactures military equipment utilized to defend US national security. However, significant risks to security and resilience of the CMS continue to evolve. These risks include actions happening on the world stage as well as actions within numerous dependent and interdependent sectors. These risks must be addressed as the CMS is a critical contributor to US national security and economic vitality.

Cross-References

- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector
- ▶ Critical Infrastructure Protection
- ▶ Department of Homeland Security (DHS)

References

Bennett, C. (2016). DHS: Cyberattacks on critical manufacturing doubled in 2015. *The Hill.* Retrieved from http://thehill.com/policy/cybersecurity/266081-dhs-critical-manufacturing-cyberattacks-have-nearly-doubled

Coullahan, B. (2017). Unmanned aircraft systems in homeland security. In R. Baggett, C. Foster, & B. Simpkins (Eds.), *Homeland security technologies for the 21st century* (pp. 149–174). Santa Barbara: Praeger Security International.

Executive Office of the President. (2013). *Presidential policy directive 21: Critical infrastructure security and resilience*. Washington, DC: Executive Office of the President.

Executive Office of the President. (2017). *Executive order 13806: Assessing and strengthening the manufacturing and defense industrial base and supply chain resiliency of the United States*. Washington, DC: Executive Office of the President.

Government Accountability Office. (2015). *Critical infrastructure protection: Sector-specific agencies need to better measure cybersecurity progress (GAO-16-79)*. Washington, DC: Government Accountability Office.

Interagency Security Committee. (2015). *Planning and response to an active shooter: An interagency security committee policy and best practices guide*. Washington, DC: U.S. Department of Homeland Security, Interagency Security Committee.

National Institute of Technology. (2015). *Framework for improving critical infrastructure cybersecurity (version 1.1, draft 2)*. Gaithersburg: National Institute of Technology.

Parfomak, P. (2008). *Vulnerability of concentrated critical infrastructure: Background and policy options*. Washington, DC: Congressional Research Service.

U.S. Computer Emergency Readiness Team. (2017). *Alert (TA17-293a): Advanced persistent threat activity targeting energy and other critical infrastructure sectors*. Washington, DC: U.S. Department of Homeland Security/U.S. Computer Emergency Readiness Team.

U.S. Department of Homeland Security. (2014). *Sector risk snapshots*. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. (2015a). *Critical manufacturing sector-specific plan: An annex to the NIPP 2013*. Washington, DC: U.S. Department of Homeland Security.

U.S. Department of Homeland Security. (2015b). *Critical manufacturing sector cybersecurity framework implementation guidance*. Washington, DC: U.S. Department of Homeland Security.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act (Public Law 107–56). 2001, October 26.

Further Reading

Baggett, R., & Simpkins, B. (2018). *Homeland security and critical infrastructure protection* (2nd ed.). Santa Barbra: Praeger Security International.

Lewis, T. (2014). *Critical infrastructure protection in homeland security: Defending a networked nation* (2nd ed.). Hoboken: Wiley.

U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. Washington, DC: U.S. Department of Homeland Security.

Critical Infrastructure: Defense Industrial Base Sector

Nagaraj S. V.[1] and Navneet Bhushan[2]
[1]School of Computing Science and Engineering, VIT, Chennai, India
[2]Crafitti Consulting, Bengaluru, India

Keywords

Critical infrastructure · Defense industrial base sector

Definition

The Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c (e)) (GPO 2010) defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The US Department of Homeland Security (DHS 2019a) defines the defense industrial base sector as "the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet US military requirements." This sector is one of the 16 critical infrastructure sectors vital to the United States.

Introduction

Former US President Barack Obama issued the Presidential Policy Directive PPD-21 in Feb 2013 (PPD-21 2013). The subject of the directive was critical infrastructure security and resilience. This directive revoked an earlier directive viz. the Homeland Security Presidential Directive/HSPD-7. PPD-21 identified 16 critical infrastructure sectors. One of these sectors is the defense industrial base (DIB) sector which is focused here.

The key objective of PPD-21 (PPD-21 2013) was to fortify and preserve "secure, functioning, and resilient critical infrastructure." The term critical infrastructure has already been defined earlier under Definitions. PPD-21 defined the terms secure and resilience. According to PPD-21 (PPD-21 2013), the term secure refers to "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." The term resilience means "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents" (PPD-21).

The DIB sector is a critical infrastructure sector, hence it becomes necessary to fortify and preserve it as stipulated by PPD-21.

Sector Overview

The Defense Industrial Base (DIB) sector supplies goods and services that are indispensable to US military operations (DHS 2019a). This sector accommodates firms executing outright under the US Department of Defense (DoD), its contractors who may enter into subcontracts, and firms furnishing materials and services. A good overview of the DIB sector is provided by a video and its transcript at a website containing information related to the Department of Homeland Security (DHS 2019b).

The DIB sector is quite unlike and as a matter of fact substantially different from other critical infrastructure sectors. This is mainly because the DIB is determined by the stakeholder instead of by goods and services. The sheer magnitude and multifariousness of the DIB sector ensues in new dimensions. For example, the DIB sector has an inordinately large and composite aggregation of industrial locations and manipulators. These locations and manipulators in fact span "15 subsectors and more than 90 segments governed by multiple regulations, laws, treaties, and precedents" (DHS 2019b). The 15 subsectors include industries related to shipbuilding, aircraft, missiles, space, combat vehicles, ammunition, weapons, troop support, information technology, electronics, and commodities related to industries pertaining to electronics, electrical, mechanical, and structural engineering, and also research and development facilities (DHS 2019b).

The facilities and installations that are present in the DIB sector are often dissimilar from one another. This means that uniform risk assessments are indeed not really feasible. As a result, defense-related commercial enterprises therefore place substantial focus on defending their assets and functions. As a consequence, the DIB sector has assigned priorities for partaking data and formulating appraisal and security processes that are enforced throughout the sector. Many programs have been specially designed to address various challenges that are thrown up. For example, the Defense Critical Infrastructure Program (DoD 2019) discovers, evaluates, and increases security around assets essential for executing the US National Military Strategy. Mission Assurance Assessments are also used to enforce critical infrastructure and key resource protection approaches.

Nowadays, cyber security has become a major universal problem. This has undoubtedly been hastened by the universal digitization of information. This has brought in a big risk of exposure or danger to unclassified program information controlled by the DoD. This could in turn nullify technological superiority and combat readiness and potential of the United States. Consequently, the DIB Cyber Security/Information Assurance Task Force was launched under an authorization from the Deputy Secretary of Defense. This was done to extenuate cyber risk to acquisition programs by defending Department of Defense-controlled unclassified information on corporate

networks in the unclassified sector. Additional measures have also been taken. To illustrate, the Defense Security Information Exchange, which is a sub-council of the DIB Sector Coordinating Council constitutes several defense contractors who apportion cyber threat and cautionary information. The DIB Cluster Buffer Zone Protection Program Pilot named geographical hubs where many critical assets are clustered. This program received a Buffer Zone Protection grant through the Federal Emergency Management Agency. The FY 2010 Buffer Zone Protection Program proved to be beneficial. Through the abovementioned initiatives and other measures of a similar nature, the DIB sector partners work collectively in order to preserve and raise the protective strength of the sector while safeguarding the United States.

Sector-Specific Agency

Sector-specific agencies are US government departments and authorities identified under the Homeland Security Presidential Directive 7/HSPD 7 and its successor PPD-21 for taking care of the particular critical infrastructure sector. The Department of Defense serves as the sector-specific agency for the DIB sector.

Sector Partners

According to the Department of Homeland Security (DHS 2019a), the DIB partnership consists of Department of Defense components, over one hundred thousand DIB companies, and necessarily even their subcontractors, all of them perform under contract to the Department of Defense. The partnership also includes "companies providing... [accompanying] materials and services to the Department of Defense... [in addition to] and government-owned/contractor-operated and government-owned/government-operated facilities... [and] domestic and foreign entities... with production assets ... [situated in several] countries" (DHS 2019a).

The DIB sector implements the National Infrastructure Protection Plan (NIPP) (refer DHS (2010) and DHS (2013)) by bettering industry security. This is achieved through joint activities with several security partners including defense industry associations and agencies traversing various levels of government. There are two main councils which make the task of coordination achievable and pragmatic. They are:

- Government Coordinating Council (GCC)
- Sector Coordinating Council (SCC)

Government Coordinating Council

This council ensures harmonious operations of various DIB sector security schemes, courses of action, and naturally intercommunication throughout and among the government and DIB security partners with the aim of supporting the national security goals of the United States.

Sector Coordinating Council

The DIB Sector Coordinating Council serves to network private sector owners or operators to work together with many government authorities for critical infrastructure protection. This council offers a single point of contact for interaction on a broad range of sector-specific infrastructure protection actions and matters. Many major private sector companies and associations are members of this council. The key focus areas of this council include:

- Information and Cyber Security
- Information Sharing
- Risk Management
- Personnel and Physical Security

Sector Dependencies and Interdependencies

Many of the 16 critical infrastructure sectors share common attributes with other critical infrastructure sectors. The DIB sector is therefore not an exception. This sector has many things in common with other critical infrastructure sectors, for example, with sectors such as "communications, critical manufacturing, energy, information technology, and transportation systems" (see DHS 2019b). The connections between the DIB sector

and the abovementioned sectors are briefly illustrated below:

DIB Sector and the Communications Sector

The DIB sector is obviously dependent on communications to fulfill much of its operations. For instance, two or more subcontractors of the DoD may wish to communicate and collaborate for fulfilling an upcoming highly confidential order. The Secretary of Defense may perhaps wish to accomplish national command authority functions, intelligence functions, and also share information with commanders. Hence, any major or severe breakdowns of communications could have a cumulative and deleterious effect on other critical infrastructure sectors as well. Thus, it becomes important to safeguard communication facilities against attacks; this includes attacks by physical means as well as through cyber means. The DoD accomplishes this task by protecting the United States from the harmful effects of these attacks by forewarning relevant organizations.

DIB Sector and the Critical Manufacturing Sector

The DIB sector and the critical manufacturing sector by design have a number of common features as well as interdependencies. These two sectors are primarily production sectors since they are essentially based on assets. The diverse assets make commodities that move within the sector, and mutually add to the further yield of each sector.

DIB Sector and the Energy Sector

PPD-21 named the energy sector as being singularly vital because that sector is absolutely necessary for other critical infrastructure sectors. However, regrettably, a significant proportion, in fact, more than 80% of the US energy infrastructure is controlled by the private sector. This effectively means that the US government has virtually little hold on that sector. However, the energy sector is undoubtedly cognizant of its exposures to malicious attacks and is therefore guiding a substantial conscious attempt to step-up preparation and readiness. Active help from industry has led to significant sharing of good practices throughout the sector. Numerous private energy sector proprietors and manipulators have in fact gained wide experience with infrastructure protection. Computerization and networking have brought many benefits but also significant threats to the energy sector. Thus, the focus of the energy sector has recently been on tackling threats due to deficient cyber security.

Nowadays, nuclear energy plays a significant role in the energy sector. The US Department of Energy works to increase national security through the military application of nuclear energy. It provides the US navy with dependable, militarily effective nuclear propulsion plants and guarantees their continued safe and steady-going operation.

DIB Sector and the Information Technology Sector

The DIB sector is an asset-based production sector, so it is contingent upon information that stays on and runs in a free manner among several government and often even corporate IT networks and systems. Needless to say, vital technology information, proprietary design information, information concerning military potentiality necessities, and so on must be coordinated and contemporized. Consequently, reliability, confidentiality, integrity, and availability of information are very crucial for DIB sector operations and hence their overall effectiveness.

DIB Sector and the Transportation Systems Sector

The DIB sector uses airway, seaway, railway, highway, and waterway networks to move equipage to assist the activities of the armed forces. Hence, the transportation sector is clearly very vital for the DIB sector. Thus, detrimental attacks on transportation networks through air, sea, or land must be prevented without any lapse.

Why Is the DIB Sector Vital to the United States?

As mentioned earlier, the DIB sector is one of the 16 critical infrastructure sectors. Hence, according to the Critical Infrastructures Protection Act of 2001 (GPO 2010), “the sector’s systems

and assets, whether physical or virtual, are vital to the United States. The incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Plans Specific to the DIB Sector

Each of the 16 critical infrastructure sectors has a sector-specific plan that pinpoints the application of the National Infrastructure Protection Plan (NIPP) (DHS 2010) model for the specific features of that sector. Thus, in the year 2010, a plan (see DHS 2010) was prepared for the DIB sector. This plan describes how the 2009 NIPP risk management fabric is applied for the DIB sector. The DIB Sector-Specific Plan of 2010 is in fact an extension to the National Infrastructure Protection Plan of the year 2009. This particular plan provided a model for an organized national endeavor to protect critical infrastructure. It ensured the inclusion of various tiers of the government, the private sector, the academic world, and even international organizations and associates. The National Infrastructure Protection Plan of the year 2009 has been superseded by the NIPP of the year 2013 (see DHS 2013). The main goals of this revised plan include protection of critical infrastructure assets, key resources, and ensuring resiliency. Needless to say, the plan of the year 2013 attempts numerous improvements to the earlier plan of 2009. This is achieved by taking note of several changes to the risks, policies, and operating environments of critical infrastructures. The revised plan also takes care of the requisites of integrating the cyber, physical, and human elements of critical infrastructure for managing risk. Its emphasis is on collaboration for managing risk and steps to be taken for advancing the national efforts for protection of vital infrastructure.

Protective Programs and Initiatives

As mentioned earlier, in the section that provides an overview of the DIB sector, the DIB sector partners place considerable emphasis on defending their assets and functions. A cornerstone of best practices thus helps to formulate sector-wide security programs beneficial for businesses of all extents and types pertinent to the DIB sector. Some of the major initiatives within the sector are listed below:

The Defense Critical Infrastructure Program (DoD 2019a) aims to guarantee that assets, especially those that are networked and crucial to DoD military missions, are always available when needed. Actions under this program admit the recognition, judgment, and security improvement of assets indispensable for accomplishing the US National Military Strategy.

Mission Assurance Assessments garner and put through critical infrastructure protection approaches.

The Defense Industrial Base Cyber Security/Information Assurance Task Force, the Defense Security Information Exchange, and organizations such as the Critical Infrastructure Partnership Advisory Council (CIPAC) and various committees are utilized for apportioning crucial information.

The Defense Industrial Base Cluster Buffer Zone Protection Program (BZPP) archetype was enforced to apportion information related to menaces, exposures, and plans for extenuation. The BZPP named DIB geographic hubs where multiple DIB critical assets were clustered. The pilot program led to Federal Emergency Management Agency BZPP grants for enhancing the readiness potentialities of communities near high-priority crucial assets.

Incident Management in the DIB Sector

Emergency Support Functions (ESFs) (DHS 2019c) are mainly used by the US government for organizing and supplying sources of aid and/or support that may be drawn upon when needed, primarily for efficient incident management during emergencies. ESFs are essentially the aggregation of capabilities of various government organizations and if necessary some private sector organizations for multiple purposes. For example, they may be used for providing resources and support, for ensuring implementation of programs and services that are much needed for saving

lives, for protecting property and the environment, and also for reestablishing essential services and critical infrastructure. Emergency Support Functions are basically intended to help victims and communities return to normal following inevitable happenings within the nation. ESFs align classes of sources of aid and purvey important aims for their use. ESFs employ resource management constructs before, during, and after an incident. For ease of execution during emergencies, several coordinators, primary agencies, and supporting agencies have already been clearly identified for emergency support functions. In the context of the National Response Framework, which is essentially a guide to how the nation responds to all types of disasters and emergencies, the US DoD is considered to be a support agency for all emergency support functions. The National Response Framework is a part of the National Strategy for Homeland Security.

The DIB sector acts upon many ESFs during incidents in order to address the concerns of industry. Associated ESFs are also available if required. Adverse incidents impacting the DIB necessitate appropriate response and risk management. The DoD has to share incident information on risks to DIB assets through appropriate federal and commercial channels. It is important for the DoD to take efforts to restitute impaired critical DIB assets irrespective of their location.

Sector Goals and Priorities

Sector Goals

The DIB sector attempts to assure it has the power to endorse DoD missions and do away with undesirable risk to national security. In order to attain this, the DIB sector partners have established five strategic goals (DHS 2019b):

- Employ an all-hazards mechanism to deal with risks related to reliance on critical sector assets.
- Ameliorate coaction in the circumstance of statutory, regulatory, proprietary, and other pertinent information-sharing constraints and guidance.
- Extenuate risk created by personnel with unaccompanied physical or logical access to critical sector assets.
- Handle risk created by menaces to and exposures of critical sector physical assets.
- Take care of risk to information that identifies or describes characteristics or capabilities of a critical DIB asset or by the nature of the information would represent a high risk/high impact to the critical infrastructure or the DIB asset.

Sector Priorities

The DIB sector is to a significant extent made up of privately owned and controlled businesses. As mentioned earlier, there is no sector-wide requirement for standardized risk assessments, although the DIB sector is subject to a variety of risk assessments in the areas of business operations, information security, and information assurance. It is indeed vital for all DIB businesses to invest in high-tech security and programs, notwithstanding the fact that they are often complicated in structure and to a great extent constantly high priced.

The DIB sector has assigned priorities to requirements to jointly apportion information and formulate appraisal and security processes that may be carried out throughout the sector. Toward that goal, the sector is progressing as indicated below (DHS 2019b):

- Moving aggressively to adapt longstanding stakeholder–vendor relationships to support the NIPP partnership model
- Conducting critical infrastructure assessment of sector assets, systems, networks, and functions
- Building a foundation of frequent communications between sector partners and the government

Sector-Specific Resources

Legislation

The Critical Infrastructure Information Act of 2002 (CII Act) (DHS 2019d) seeks to help better sharing of critical infrastructure information among the proprietors and operators of the critical infrastructures and also the government entities

with infrastructure protection obligations. This helps reduce United States vulnerability to terrorism. The Act (DHS 2019d) "consists of a group of provisions that address the circumstances under which the Department of Homeland Security may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program." The US Congress has set standards for defending critical infrastructure information by means of the CII Act of 2002. In response, the Department of Homeland Security produced the Protected Critical Infrastructure Information program (CISA 2019). The aim of this program is to guard crucial substructure information freely portioned out with the government for US national security aims. The program is also a fundamental part of efforts undertaken to defend the United States critical infrastructure from cyber-attacks.

Directives

Several directives relate to the DIB sector. A case in point is the Department of Defense Directive 3020.40 (DHS 2019d) "updates policy, and assigns responsibilities for the Defense Critical Infrastructure Program." In addition, the Homeland Security Presidential Directive 7/HSPD 7 and its successor PPD-21 laid down a national policy for government departments and agencies to distinguish and assign a priority to US critical infrastructure and key resources and to defend them from extremist attacks. Additional relevant directives include the (DHS 2019d):

- DoD Directive 5000.1 ("The Defense Acquisition System")
- DoD Instruction 5000.2 ("Operation of the Defense Acquisition System")
- DoD Directive 5000.60 ("Defense Industrial Capabilities Assessments")

Training

Many DoD agencies, academies, and organizations provide training, security education, and the ability to respond to disasters as well as emergency situations. The training is available for first responders and others. The training also provides formal instruction and counseling in assessing, identifying, and prioritizing homeland security measures.

Publications

Several publications related to the DIB sector are available (DHS 2019b). An example of such a publication is the DoD's DIB Defense Sector Assurance Plan, which furnishes a well-organized scheme for dealing with risk to industrial potentialities at critical asset locations situated all over the world. DoD has also published its "Defense Critical Infrastructure Program Infrastructure Resilience Guide," which serves as an aid to people who review infrastructure dependencies and develop and implement mitigation measures. Moreover, the Government Accountability Office published a manual, titled "Defense Infrastructure: Management Actions Needed to Ensure Effectiveness of DoD's Risk Management Approach for the Defense Industrial Base," which identified and evaluated DoD's "risk management approach to ensur[ing] the availability of DIB assets, and... identified challenges the DoD faces in its approach to risk management" (GAO 2017). Furthermore, the National Defense Industrial Association provides links to related studies, reports, and proceedings, and publishes the National Defense magazine.

Executive Order 13806

Successive US Presidents have been very keen in strengthening the manufacturing and DIB as well as the supply chain resiliency of the United States. As mentioned before, former US President Barack Obama issued the Presidential Policy Directive PPD-21 (PPD-21 2013) in Feb 2013, the subject of which was critical infrastructure security and resilience. In the year 2017, in the month of July, US President Donald Trump brought out Executive Order 13806 (White House 2017). This order was for evaluating and toughening the manufacturing and DIB and supply chain resilience of the United States.

In order to comprehend some of the issues currently faced by the DIB sector, it is instructive to study Executive Order 13806. This order mentions that the fabricating capability and DIB of

the United States have been diminished by the deprivation of over sixty thousand factories and almost five million fabrication jobs since the year 2000. It also remarks that workforce skills are important to national defense. The executive order emphasizes the need for producing "education and workforce development programs and policies that support job growth in manufacturing and the" DIB (White House 2017). The order further called for an evaluation of the DIB and supply chains, with comments from multiple administrative departments and agencies in order to allow for an absolutely needed and indispensable assessment of the current strengths and weaknesses. The assessment as requested by the executive order was published in September 2018 (DoD 2018).

The Assessment Report Produced in Response to Executive Order 13806

An interagency task force submitted an unclassified publicly accessible report (DoD 2018) in September 2018 to US President Donald Trump in fulfillment of the Executive Order 13806 of July 2017. The report which is very informative has the following major findings (DoD 2018):

- Macro forces have contributed to substantial consequences chiefly in the sublevels of the defense supply chain.
- An amazing level of dependence on rival countries subsists.
- Employers across all sectors face manpower challenges.
- A large number of sectors are actively shifting critical potentialities abroad in quest of more lucrative pricing and also for entry into foreign markets.

The assessment report begins with an overview of America's manufacturing and DIB. It then lists five macro forces forcing risk into America's industrial base (DoD 2018):

(i) Sequestration and doubtfulness of US government expenditure
(ii) Reduction of US manufacturing capability and capacity
(iii) Detrimental US government business and procurement activities
(iv) Industrial action plans of rival nations
(v) Declining US Science, Technology, Engineering, and Math (STEM) and trade capabilities

Table 1 elucidates these forces (see Fig. 7 of the report):

Ten risk archetypes threatening America's manufacturing and DIB are then mentioned in the report. Table 2 (see Fig. 23 of the report) illustrates them:

The impacts of these risk archetypes on America's industrial base are noted. These include:

- Scaled down investment in new capital as well as research and development
- Consequent decreases in the rates of modernization and technical creation
- A deprivation of providers and possible chokepoints throughout the numerous tiers of the supply chain
- More depleted quality and above normal prices ensuing from trimmed down competition

An important point to note is that the impacts identified in the assessment report (DoD 2018) often fell into multiple risk archetypes. For example, "a financially distressed foundry may be both a sole source and single source, as well as illustrate a fragile market" (DoD 2018). The assessment report gives a summary of demonstrative examples in each of the risk archetypes. A broad list of about 300 impacts for all the 16 critical infrastructure sectors was made available in a classified appendix to the report.

A Blueprint for Action

The assessment report (DoD 2018) produced in response to Executive Order 13806 (White House 2017) includes a blueprint for action. The blueprint makes a note of current efforts and lists

Critical Infrastructure: Defense Industrial Base Sector, Table 1 Macro forces

Macro forces	Explanation
Sequestration and uncertainty of US government spending	Discrepant appropriations, doubts about succeeding national budgets, macrolevel equivocalness in US government outlays, and the consequences of the budget control act make markets precarious
Decline of US manufacturing base capabilities and capacity	Diminutions throughout the fabricating and defense industrial base of the United States impact the usefulness of providers, overall capability, and capabilities operational across the country
Deleterious US government business and procurement practices	Demanding situations when dealing with the DoD and other US government clients, including contractual arrangements, ordinances, policies, roadblocks to involvement, qualification disputes, alterations of plans, and other troubles can contribute to untoward impressions on providers
Industrial policies of competitor nations	The national industrial policies and the external trade policies of rival nations, particularly the economic aggressiveness of China, bring down the usefulness, capabilities, and capacity of the US National Security Innovation Base
Diminishing US STEM and trade skills	Disruptions in US human capital, in particular a deficiency of STEM natural endowments and worsening trade skills decrease national capacity to develop something new, fabricate, and uphold

Source: Fig. 7 of DoD (2018).

Critical Infrastructure: Defense Industrial Base Sector, Table 2 Risk archetypes threatening America's manufacturing and DIB

Risk archetype	Occurs when
Sole source	Just one supplier is in a position to furnish the needed capability
Single source	Just one supplier has measured up to stipulated norms to furnish the needed capability
Fragile supplier	A particular supplier is in a state of woe from a financial point of view
Fragile market	The economics of an industry are not robust and the possibility of nearing liquidation is imminent
Capacity-constrained supply market	Capacity is out of stock in wanted amounts or time due to vying market requirements
Foreign dependency	The national industry does not make the product or does not make it in ample amounts. Hence, there is dependence on foreign sources
Diminishing manufacturing sources and material shortages	Product or material devolution ensuing from slump in germane providers
Gap in US-based human capital	The industries in the United States are not in a position to employ or retain workers with the desired skill sets due to manpower shortages
Erosion of US-based infrastructure	Expiration or obsoleteness of specified capital equipment required to incorporate, fabricate, or preserve capability
Product security	Deficiency of cyber and physical safety ensues in degradation of unity, assurance, and competitive benefits

Source: Fig. 23 of DoD (2018).

future efforts and recommendations. The recommendations include (DoD 2018):

- Creating an industrial plan of action endorsing national security efforts
- Amplifying direct investment in the bottom levels of the industrial base and programs to deal with decisive chokepoints, patronize delicate suppliers and extenuate single points-of-failure

- Branching out from everlasting reliance on sources of supply in politically fluid countries who may interrupt access by the United States
- Working together with friendly nations and collaborators on articulated industrial base challenges
- Modernizing the organic industrial base
- Accelerating workforce development efforts
- Reducing the personnel security clearance backlog
- Enhancing efforts exploring next generation technology for future threats

Conclusion

The defense industrial base sector is a critical infrastructure sector which needs to be fortified and preserved. The differences between the DIB sector and other sectors arise because the DIB is defined by the stakeholder. The DIB sector has an incredibly large number of partners which adds to its complexity. It has many dependencies and interdependencies with other critical infrastructure sectors. The DIB sector is very vital to the United States and many sector-specific plans have evolved and continue to evolve. A number of initiatives and protective programs have been launched to safeguard the DIB sector. Executive Order 13806 has had a major effect in revitalizing the DIB sector. Numerous challenges need to be addressed and these can be handled if appropriate measures are taken right away as suggested by the assessment report produced in response to the order.

Cross-References

- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure Protection
- ▶ Department of Homeland Security (DHS)

References

Department of Defense (DoD). (2018). Assessing and strengthening the manufacturing and defense industrial base and supply chain resiliency of the United States – Report to President Donald J. Trump by the interagency task force in fulfillment of executive order 13806. Available at https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/assessing-and-strengthening-the-manufacturing-and%20defense-industrial-base-and-supply-chain-resiliency.pdf Accessed 25 June 2019.

Department of Defense (DoD). (2019). Defense critical infrastructure program. Available at https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-Global-Security/Defense-Critical-Infrastructure-Program/ Accessed 25 June 2019.

Department of Homeland Security (CISA). (2019). Cyber security and infrastructure security agency, protected critical infrastructure information program. https://www.us-cert.gov/pcii Accessed 25 June 2019.

Department of Homeland Security (DHS). (2010). The 2010 defense industrial base sector-specific plan. Available at https://www.dhs.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf Accessed 25 June 2019.

Department of Homeland Security. (2013). The national infrastructure protection plan 2013. Available at https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf Accessed 25 June 2019.

Department of Homeland Security. (2019a). Defense industrial base sector. Available at https://www.dhs.gov/cisa/defense-industrial-base-sector Accessed 25 June 2019.

Department of Homeland Security. (2019b). Understanding the defense industrial base sector. http://www.humtech.com/fema/CI_RC/defense1.htm Accessed 25 June 2019.

Department of Homeland Security (DHS). (2019c). Federal emergency management agency, emergency support functions, https://www.fema.gov/media-library/assets/documents/25512 Accessed 25 June 2019.

Department of Homeland Security (DHS). (2019d). Critical infrastructure information act of 2002. https://www.dhs.gov/sites/default/files/publications/CII-Act-508.pdf Accessed 25 June 2019.

Government Accountability Office (GAO). (2017). Defense infrastructure: management actions needed to ensure effectiveness of DOD's risk management approach for the defense industrial base. GAO-07-1077. https://www.gao.gov/assets/270/265836.html

Government Publishing Office (GPO) (US). (2010). 42 U.S.C. 5195c (e)). Available at https://www.govinfo.gov/content/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf Accessed 25 June 2019.

Presidential Policy Directive PPD-21. (2013). Available at https://obamawhitehouse.archives.gov/the-press-office/

2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil Accessed 25 June 2019
White House. (2017). Executive order 13806. Available at https://www.whitehouse.gov/presidential-actions/presidential-executive-order-assessing-strengthening-manufacturing-defense-industrial-base-supply-chain-resiliency-united-states/ Accessed 25 June 2019.

Further Reading

Baggett, R. K., & Simpkins, B. K. (2018). *Homeland security and critical infrastructure protection* (2nd ed.). Santa Barbara, CA: Praeger Security International.
Lewis, T. (2014). *Critical infrastructure protection in homeland security: Defending a networked nation* (2nd ed.). Hoboken, NJ: Wiley.

Critical Infrastructure: Emergency Services Sector

Brian Keith Simpkins
Homeland Security Program, Eastern Kentucky University, Richmond, KY, USA

Keywords
Dependencies · First Responder · Interdependencies · Natural Hazards · Risk Profile

Definition

Critical Infrastructure	"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism [USA PATRIOT] Act 2001).
Emergency Services Sector	The Emergency Services Sector (ESS) provides services to all five mission areas defined in the National Preparedness Goal: prevention, protection, mitigation, response, and recovery (U.S. Department of Homeland Security [DHS] 2015c). The services are provided by career and volunteer first responders and associated capabilities and resources across the county at the federal, state, and local levels as well as the private sector (U.S. Department of Homeland Security [DHS] 2015a).

Introduction

Each and every day, the Emergency Services Sector (ESS) plays an important role in safeguarding lives and property across the United States. Although the ESS responds when assets in other critical infrastructure sectors need assistance, the sector itself faces challenges to security and resilience. Some of the risks faced by the ESS are similar to other infrastructure sectors, such as a changing threat and hazard picture, climate change, and cyber-attacks through increased reliance on Internet-connected systems. These high-level challenges are just the beginning as the ESS faces a myriad of other risks related to natural hazards, technological hazards, and human-caused incidents. This is in addition to dependencies and interdependencies with other infrastructure sectors, which can result in significant cascading effects.

The remainder of this entry provides a general overview of the ESS to enable a general understanding. Within the discussion, key operational characteristics of the ESS are reviewed along with a description of the current risk profile to include critical cross-sector dependencies and interdependencies. This discussion will also include vision/mission, goals, and priorities of the ESS along with the partnership structure. Partnerships and

information sharing within the ESS have extreme importance in order to address and respond to human-caused incidents that can result in significant casualties and damage to infrastructure assets. Overall, this entry provides a basic understanding of the ESS to enable critical evaluation of current policies, practices, and needed activities to address gaps in security and resilience.

Sector Overview

The ESS has the primary protection responsibility of other critical infrastructure sectors and assets. The ESS is the first line of defense for all mission areas (prevention, protection, response, recovery, and mitigation) related to natural hazards, technological hazards, and human-caused incidents that may affect infrastructure assets. To accomplish this task, the ESS consists of millions of highly skilled first responders (human element) along with physical and cyber assets/elements. Consisting of both paid and volunteer forces, the ESS is organized/structured at the federal, state, local, tribal, and territorial levels of government. Therefore, ESS agencies include the primary public first responder agencies at each government level. ESS assets also include personnel and associated resources within the private sector such as private security and fire/emergency medical services at industrial sites. Due to the focus on the protection of other infrastructure sectors and assets, the ESS faces distinctive challenges in security and resilience of ESS assets, such as communications and data networks. The disruption of physical or virtual ESS assets can result in significant consequences to public safety and security.

Sector Components and Assets

The ESS has components related to the human, physical, and cyber elements. For human, the ESS is comprised of paid and volunteer individuals within the primary response disciplines. For physical, this realm includes ESS facilities from which daily operations are administered as well as facilities that support training and storage. Additional physical assets include equipment (e.g., personal protective [PPE], communications, and surveillance equipment) and vehicles (e.g., ambulances, patrol vehicles, fire apparatus, aircraft, and watercraft) that are specialized for specific disciplines and for capability. In regard to cyber, this element includes operational communications (e.g., two-way radio systems), databases (e.g., criminal record databases), management (e.g., incident decision support software), biometric systems, security systems, and information networks (e.g., computer-aided dispatch [CAD]). Aside from human, physical, and cyber realm, the ESS is officially compartmentalized into five distinct emergency responder disciplines or subsectors as described below per the *Emergency Services Sector-Specific Plan* (ES SSP).

Law Enforcement: Consists of police departments, sheriff's offices, courts systems, correctional institutions, and private security agencies. Provides services such as enforcing laws, conducting criminal investigations, collecting evidence, apprehending suspects, securing the judicial system, and ensuring custody and rehabilitation of offenders.

Fire and Rescue Services: Consists of both paid and volunteer personnel. Provides services such as fire suppression, fire prevention, hazardous materials control, life and property safety operations (including technical rescue), building code enforcement, and fire safety education.

Emergency Medical Services: Provides services at incidents such as triage, treatment, and transport of injured and ill patients; taking appropriate steps to protect staff, patients, facilities, and the environment; and helping to monitor response teams while providing needed comprehensive medical care to patients.

Emergency Management: Provides incident management and coordination (including pre- and postevent activities) between ESS disciplines, as well as with nonemergency services entities. Emergency Operations Centers (EOCs) provide emergency management personnel with the capability for multiagency coordination for incident management by activating and operating for preplanned or

no-notice events. EOCs support the coordination of response and recovery activities among neighboring jurisdictions at and all levels of government if needed.

Public Works: Provides service such as assessing and repairing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris from public spaces; restoring utility services; and managing emergency traffic. With responsibility for hardening security enhancements to critical facilities and monitoring the safety of public water supplies, public works is an integral component of a jurisdiction's emergency planning efforts. In addition, public works departments supply heavy machinery, raw materials, and emergency operators and may also manage contracts for additional labor, equipment, or services that may be needed before, during, and after an incident (U.S. Department of Homeland Security [DHS] 2015a, p. 5).

In addition to the responder disciplines/subsectors, the ESS also consists of specialized personnel and teams that provide additional emergency response capability when appropriate. This specialized capability can be present in one or more of the responder disciplines/subsectors and can focus in areas such as special weapons and tactics, hazardous materials, explosive ordinance disposal, search and rescues (air, land, marine), and National Guard Civil Support (DHS 2015a).

Key Sector Operating Characteristics

As previously stated, the ESS has the primary protection responsibility of other critical infrastructure sectors and assets and acts as the first line of defense in relation to natural hazards, technological hazards, and human-caused incidents that may affect infrastructure assets. This responsibility is handled by more than 2.5 million first responders that serve in all 56 US states and territories (DHS 2015a). Decisions made by the ESS in response to incidents can affect the level of damage inflicted to infrastructure and how quickly services are restored. Although the ESS operations are required to be adaptable and flexible to address any incident, the sector does have limitations when facing incidents and disasters – or circumstances – which have not been training for or previously experienced. Overall, the graphically dispersed aspect of the ESS makes it difficult to completely disable nationwide, but this aspect also creates challenges in across government levels and responder disciplines. Further, the ESS is driven by the human element, but is dependent on the cyber element (e.g., communications, information technology) and physical element (e.g., response vehicles and equipment).

Another limitation of the ESS is limited resources, especially in ESS agencies located in small and rural communities. Not only have operational budgets within local and state ESS agencies decreased over the past decade, but federal grant funding for ESS agencies has also vastly decreased over the same time period. Limited financial budgets affect the operational capacity of ESS agencies (e.g., less personnel, use of older/outdated equipment) to address and respond to current risks and adapt to changing risks. Resource constraints are just one operational consideration of the ESS, and others include the following:

Rural and Frontier Resource Constraints: In rural and frontier communities, limited populations and smaller tax bases create difficulties and shortcomings for ESS agencies in terms of staffing, equipment, and other resources.

Geography: The ESS operates in density-populated urban environments as well as in vast and, oftentimes, sparsely populated areas, both of which provide significant challenges. For example, in rural and frontier areas, greater distances traveled and difficult on-road and off-road terrain (e.g., mountains, marshlands, wilderness) may significantly impact response planning and operations.

Infrastructure: Although urban ESS agencies may benefit operationally from an increased presence of infrastructure, it also creates more infrastructure to protect. As for rural areas, many segments of critical infrastructure, such as hospitals and other healthcare facilities, are less capable (e.g., have fewer physicians and

specialists per capita) than similar infrastructure in urban areas for various reasons. These conditions may limit response to public health hazards such as communicable diseases.

Modernization: Citizens of all communities continue to demand that ESS agencies modernize systems despite resource shortages. Today, approximately 88% of US adults own a cell phone and 78% access the Internet. ESS agencies must upgrade their own equipment as well as 9-1-1 centers, warning systems, and online resources for the benefit of their residents (Simpkins 2015, p. 3).

All of the constraints above are intensified by the fact that a majority of ESS personnel are volunteers. For example, volunteers are often assigned as county emergency managers and/or required to fully staff rural fire departments (U.S. Fire Administration 2007). This occurrence does not happen in rare circumstances. Rather, rural areas constitute 80% of the landmass and 20% of the population in the United States (McGinnis 2004). Additionally, frontier areas are classified as areas with an extremely low population density (less than six persons per square mile) and are characterized by isolation from population centers (e.g., cities) and provision of services (e.g., hospital, cell phone service), which comprise approximately 2% of the US population and 46.7% of the land within the Unites States (largely concentrated in the Western United States and Alaska) (National Center for Frontier Communities 2013).

Across the United States, ESS missions are completed by approximately 2.6 million individuals in the law enforcement, fire and rescue, emergency medical services (EMS), emergency management, and public works disciplines (DHS 2015a). This is in addition to ESS personnel within the private sector that includes industrial fire departments, corporate security operations, and private EMS providers. As for the number of rural first responders, there is no single source for a specific number. However, descriptive information can be gleaned from various sources. For example, the National Institute of Justice (2004) reports that approximately 90% (or ~14,500) of the over 16,000 municipal and county law enforcement agencies in the United States serve populations under 25,000 and over half of all agencies employ 10 or fewer officers. Further, the US Fire Administration (2007) reports that 44% (or ~13,440) of the over 30,000 fire departments in the United States are located in rural areas.

Similar to other critical infrastructure sectors, the ESS is not heavily regulated, but specific regulations govern or provide reference for use in emergency response operations (e.g., hazardous materials incidents), responder safety (through the Occupational Safety and Health Administration [OSHA], and professional codes and standards for fire prevention and public safety (through the National Fire Prevention Association [NFPA]). Despite limited regulation, the agencies across the ESS rely heavily on communications and information technology networks during incident response. Protecting these networks is essential for ESS agencies to support critical infrastructure security and resilience as well as to ensure the provision or quick restoration of essential public services and infrastructure assets.

Sector-Specific Agency

The US government by itself cannot create a secure and resilient ESS. Rather, the end goal requires a dedicated whole-of-nation approach involving public and private stakeholders. Leading this whole-of-nation approach is the designated Sector-Specific Agency (SSA) as defined in *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience*. The designated SSA for the ESS is DHS. More specifically, the Office of Infrastructure Protection is the delegated responsible entity within DHS.

Sector Partnerships

Security and resilience of the ESS requires a broad spectrum of partnerships to facilitate information sharing and situational awareness to address sector risks. Specific partnership structures are defined within the ES SSP. However, the ESS utilizes the *National Infrastructure Protection Plan* (NIPP) partnership structure and additional collaboration mechanisms based on Government

Coordinating Councils (GCC) and the Sector Coordinating Councils (SCC). Beginning with the SCCs, these councils are comprised of owners and operators who utilize the council to directly collaborate with one another. Typically organized under subsectors within an overall infrastructure sector, SCCs are self-organized, self-run, and self-governed councils and serve as principal collaboration points between the GCCs and the SSAs. Conversely, the GCC focuses on collaboration and information sharing between the SSA, or federal departments and agencies, and state, local, tribal, and territory (SLTT) agencies. Members of the GCC and the SCC utilize collaborative mechanisms, such as the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate collaboration and information sharing across the public and private sectors. These collaborative partnerships and subsequent information sharing are crucial to achieving infrastructure security and resilience. This enables public and private entities to freely share information to identify mutual risks and potential solutions that benefit entire sectors. Through the defined partnership structures of the ESS, overall security and resilience posture of the sector can be continuously improved.

Sector Risks

Despite the diverse collection of assets within the ESS, common risks exist that the sector must address. Climate change, extreme weather, terrorism, and malicious actors are persistent risks across the ESS (DHS 2014). Further, cyber vulnerabilities continue to increase as reliance on networked systems continues to rise in an effort to increase efficiency and cost-effectiveness. Some of these threats are more pronounced in the ESS due to the need for open public access and the responsibility to respond to any incident. This illustrates the need to comprehensively examine risks across the ESS through existing partnership structures in an effort to ensure security and resilience. Although numerous risks can be discussed, the following sections focus on those risks deemed significant. It is acknowledged there are other significant risks to the ESS, such as the loss of two-way communications. However, these risks will not be discussed for the sake of brevity. Expanded information on risks to the ESS is accessible via the ES SSP.

Cyber Risks

The cyber threat is common throughout all critical infrastructure sectors including the ESS. Information networks and other technology resources are vulnerable to various types of attacks, which continue to increase in occurrence and severity thereby resulting in significant risk to the ESS (DHS 2012, 2015b; U.S. Government Accountability Office [GAO] 2008, 2014; Green 2016). In fact, the cyber threat is considered one of the most serious threats to all critical infrastructure sectors. Like other infrastructure sectors, the ESS is heavily dependent on cyber infrastructure and operates in a data-driven environment. Further, much of the cyber infrastructure utilizes commercial-off-the-shelf (COTS) products and systems, which have inherent vulnerabilities to malicious individuals. Individuals both inside and outside of the United States attempt to exploit the vulnerabilities, which puts current and future ESS capabilities at risk. In fact, the US Department of Defense (2011) *Strategy for Operating in Cyberspace* predicts the risk from foreign entities and non-state actors attempting to exploit cyber vulnerabilities will continue to increase in the future.

Ultimately, cyber vulnerability also poses a significant threat to the ESS sector and its ability to fight crime and complete other essential missions related to public safety and security. Most importantly is the ability to communicate, including the ability for citizens to reach ESS agencies via 9-1-1 services. More than just call centers, public-safety answering points (PSAPs) utilize information technology systems that merge phone numbers with geographic and other location data. These systems are vulnerable due to the increasing reliance on the Internet for operations, which makes 9-1-1 services susceptible to cyber-attacks. It is expected that attacks on ESS communication networks will become more frequent in the future (DHS 2015b; Green 2016). Between 2013 and 2016, over 600 critical

government phone systems and 200 PSAPs nationwide were affected by telephony denial of service attacks (Green 2016). In addition to communications, the ESS is increasingly reliant on other cyber-based infrastructure for data and information management (including cloud-based systems), biometric activities, electronic security systems, and geospatial tools. Due to this connectivity, ESS cyber infrastructure is vulnerable to cyber-attacks (e.g., denial-of-service attacks, phishing, passive wiretapping, Trojan horses, viruses, worms) from individuals and group operating around the world (DHS 2015b; GAO 2014; Green 2016).

Another common threat to all computers and networks is ransomware, which encrypts or otherwise disables access to information unless a ransom is paid (a common form of payment requested is Bitcoin). The ESS is vulnerable to this threat as illustrated by multiple ESS agencies being targets of ransomware attacks since 2014 in states such as California, Nevada, Wisconsin, and North Carolina. These attacks can disrupt initial response by ESS agencies to an incident as well as endanger first responders and members of the general public. Ultimately, the ESS is increasingly dependent upon information technology networks for multiple operations, which greatly amplifies vulnerability to cyber-related incidents.

Climate Change, Natural Hazards, and Extreme Weather

As with other infrastructure sectors, the ESS is impacted by climate change. Not only are climate change risks present; their rate of occurrence and level of severity are increasing including their effects on natural hazards. Regardless of the natural hazard/disaster or extreme weather event, the ESS is faced with sometimes unpredictable natural threats in a dynamic response environment. Increased occurrence and severity of natural hazards place increased demands on ESS assets and threaten the provision of key services. These events are increasing in terms of geographic magnitude and severity thereby requiring a surge of ESS assets for extended operational periods. A recent example is the catastrophic flooding in the Houston (TX) due to Hurricane Harvey in late August 2017. In addition to ESS response personnel, natural hazards can also impact cyber infrastructure. This impact can be significant as 9-1-1 communication networks can be disrupted. Further, impacts from natural hazards can also impact ESS operational communications networks, such as two-ways radio communications.

Two events illustrate the risk from natural hazards to 9-1-1 communication systems and operational communications networks. First, a major storm during June 2012 resulted in a total disruption of telephone services supporting 9-1-1 service across several cities and counties in Virginia (GAO 2014). The service outage was a result of loss of main commercial power and subsequent failure of a backup generator in the telephone service provider's facilities (GAO 2014). The lack of redundant measures and mitigation planning contributed to a significant disruption of public service answering points (PSAP) operations during the outage (GAO 2014). Second, Hurricane Katrina resulted in the destruction or degradation of three million landlines, 2,000 cell towers, more than 30 public service answering points (PSAPs), 37 of 41 broadcast radio stations, and first responder land mobile radio service across the region (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). Satellite phones were in short supply and unable to be charged due to lack of electrical power and fuel to run emergency generators (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). The New Orleans (LA) Police Department and the Mississippi National Guard were unable to establish effective communications for several days (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). In addition to operable communication, situational awareness was nonexistent due to a lack of interoperability between federal, state, and local communications systems (Miller 2006; Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina 2006). This illustrates that the continued increase in the occurrence and severity of natural hazards

will place demands on the ESS to mitigate operational disruptions while addressing increased public demand for service.

Epidemics and Pandemics

Evolving threats to the ESS include infectious disease occurrences, which can include diseases such as Ebola, smallpox, tuberculosis, severe acute respiratory syndrome (SARS), and Middle East respiratory syndrome (MERS) (National Infrastructure Advisory Council 2007). Infectious diseases can spread easily in today's highly mobile society and can easily morph into an epidemic (affecting a localized area) or pandemic (affecting a large region) (National Infrastructure Advisory Council 2007). A critical impact of an epidemic or pandemic is the loss of ESS personnel due to infections. Therefore, emerging and re-emerging infectious diseases must be planned for as ESS personnel would be important response assets. However, variation is persistent across the nation in terms of community fiscal health, at-risk population levels, training competencies, and countermeasure availability when addressing infectious disease epidemics and pandemics. These events can also have significant, long-term impacts on communities, especially in relation to high-risk and vulnerable populations. In fact, the United States has a constant risk of an onset of a severe influenza pandemic, and the influenza season of 2014 provides insight into the risk and how a rapidly spreading infectious disease can impact the ESS. A more concerning thought, however, is the intentional release of a more dangerous infectious disease such as smallpox and the catastrophic impacts on the nation if its spread is not readily contained.

Terrorism, Violent Extremism, and Malicious Actors

Due to the nature of their work, ESS personnel are vulnerable to human-caused incidents to include terrorism and actions by malicious actors to include active shooters. This is especially true for the ESS which perpetually faces the challenge to prepare for current threats as well as evolving threats that may require new or expanded capabilities and competencies. Further, response personnel can become targets of (secondary) attacks when responding to human-caused events in which an attacker's goal is to achieve a maximum amount of casualties. This is especially true if adversaries are targeting persons in specific authority positions or are symbolic of a social institution. Adversaries can include terrorists and violent extremists, who often target ESS personnel and symbolic targets.

Improvised Explosive Devices

The use of improvised explosive devices (IEDs) continues to be a common asymmetrical attack method by terrorists and violent extremists. Not only can IEDs damage infrastructure and cause mass causalities; they can also be used to target ESS personnel when responding to an initial incident through secondary devices. Another common practice is the simultaneous use of IEDs at multiple locations, which is specifically designed to affect ESS agency response efforts. Further, active shooter events can incorporate IEDs in an effort to increase causalities or hamper and slow down response from ESS agencies. For example, the perpetrators of the San Bernardino (CA) shooting on December 2, 2015 placed a pipe bomb in the Inland Regional Center, but was not detonated (Winton and Queally 2016). Overall, the threat of IEDs is constant across many infrastructure sectors, including the ESS.

Primary Sector Dependencies and Interdependencies

Today, critical infrastructure sectors are highly dependent and interdependent on one another through physical and cyber linkages. After a natural disaster, man-made incident, or technological accident, a significant failure in one sector – such as in the Energy Sector or Water and Wastewater Systems Sector – has the potential to cascade and create significant impacts to other regions. Currently, the ESS has dependencies on the sectors of Communications and Information Technology and interdependencies with the sectors of Energy, Transportation Systems, Water and Wastewater, Government Facilities, and Healthcare and Public Health (DHS 2014, 2015a). Descriptions of select

dependencies and interdependencies are provided below.

Communications: Provide essential services to ESS for daily operations and other activities. Of particular importance is ESS response coordination communications and public alert and warning.

Energy: Fuel and electric power are essential for operations within the ESS. This includes ESS response activities and daily business operations, movement of resources, and response coordination.

Information Technology: Provides essential services to the ESS in support of a variety of cyber-related assets and essential to operations and fulfillment of mission responsibilities. With increasing dependency on cyber-related assets and systems, disruptions or degradation of service would significantly impact the ESS, including the capability to adequately protect the public and safely and quickly respond to emergencies.

Transportation Systems: Secure and effective movement of personnel, resources, and services over multiple modes is required for the ESS. Specifically, response vehicles must be able to transport people, resources, and services to and from incident areas.

Water and Wastewater Systems: Critical for sustaining communities and infrastructure before, during, and after emergencies and is a basic human need vital to human health. For example, the ESS relies on water in response to fires and natural disasters (e.g., bottle water distribution) (DHS 2014, p. 20; 2015a, p. 4, 9–10).

In addition to external dependencies and interdependencies between sectors, the ESS also experiences internal interdependencies similar to other sectors. This is because each responder discipline within the ESS is interdependent on one another for continued functioning. For example, law enforcement secures emergency scenes for fire services and EMS to provide needed services. Additionally, public works ensures roadways are clear of debris to facilitate emergency scene access for other response disciplines. Today, the continual operation of the ESS is dependent and interdependent on other infrastructure sectors. Greater dependences and interdependencies, especially in the cyber realm related to communications and information technology, create the potential that even a localized disruption will have the ability to cascade to other sectors. This is in addition to vulnerabilities within the global and national supply chains that can pose significant disruptions to public safety and security.

Sector Vision, Goals, and Priorities

In alignment with the NIPP, each SSA develops a specific vision and/or mission for their respective infrastructure sector, which is defined in individual SSPs. Listed below are the specific vision and vision statements for the ESS.

Vision Statement: An Emergency Services Sector in which personnel and operational capabilities are prepared for and resilient to inherent and unforeseen risks; ensuring timely, coordinated all-hazards emergency response and public confidence in the sector.

Mission Statement: Save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery during emergencies (DHS 2015a, p. 26).

In addition to defining the vision and/or mission, the ES SSP identifies specific goals and priorities aligned with the five overall national goals defined in the NIPP, which are provided below.

Sector Goals

1. Continuous growth and improvement of sector partnerships to address risk mitigation and resilience efforts (*NIPP Goal #4*).
2. Support an information sharing environment for information, intelligence, and incident reporting (*NIPP Goals #4 and #5*).
3. Employ a risk-based approach to improve the preparedness and resilience (*NIPP Goal #1*).
4. Improve operational sustainability, resilience, and recovery capacities following an incident (*NIPP Goals #2 and #3*) (DHS 2015a, p. 27).

Sector Priorities

1. Utilize collaborative approaches to strengthen critical infrastructure protective planning and decision-making.
2. Develop and promote information sharing via councils and new, innovative processes and technologies to support protective programs; share risk, capacity building, and model practices information; and improve resource sharing systems and standards.
3. Identify and implement an approach/process to assess and prioritize risk and capability gaps in the ESS to enhance the resilience and recovery capabilities following an incident.
4. Develop and report metrics to measure effectiveness of efforts and gather a means to measure effectiveness (DHS 2015a, p. 27).

Conclusion

The ESS encompasses critical missions that if significantly disrupted or degraded would result in disastrous consequences to the safety and security of US citizens, protection of critical infrastructure, and overall public safety and security. For example, successful intentional cyber or physical attacks on ESS assets could impact domestic emergency response and the provision services to individuals in need. This is in addition to the ever-present risks from natural hazards, which is increasing due to climate change. Therefore, the risk profile of the ESS continues to evolve. These risks include actions happening on the world stage as well as actions within numerous dependent and interdependent infrastructure sectors. Per the NIPP, risks must be continuously evaluated and addressed, especially in the ESS due to its role in US domestic security.

Cross-References

- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Government Facilities Sector (GFS)
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector
- ▶ Critical Infrastructure Protection
- ▶ Department of Homeland Security (DHS)

References

Green, J. (2016, February 26). DHS: Hackers increasingly targeting emergency systems. WTOP. Retrieved from https://wtop.com/j-j-green-national/2016/02/dhs-hackers-increasingly-targeting-emergency-systems/

McGinnis, K. (2004). *Rural and frontier emergency medical services: Agenda for the future*. Kansas City: U.S. National Rural Health Association.

Miller, R. (2006). Hurricane Katrina: Communications and infrastructure impacts. In B. Tussing (Ed.), *Threats at our homeland: Homeland defense and homeland security in the new century – A compilation of the proceedings of the first annual homeland defense and homeland security conference* (pp. 191–204). Carlisle Barracks: U.S. Army War College.

National Center for Frontier Communities. (*2013). Population densities of frontier areas in the United States*. Retrieved from http://frontierus.org/wp-content/uploads/2014/09/2010_frontier-areas-and-pop-densities.xlsx

National Infrastructure Advisory Council. (2007). *The prioritization of critical infrastructure for a pandemic outbreak in the United States: Final report and recommendations*. Washington, DC: U.S. Department of Homeland Security, National Infrastructure Advisory Council.

National Institute of Justice. (2004). *Research for practice: Law enforcement technology – Are small and rural agencies equipped and trained*. Washington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. (2006). *A failure of initiative: Final report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina* (Report 109–377). Washington, DC: U.S. Government Printing Office.

Simpkins, B. (2015). *2014–2015 national rural training needs assessment – volume II: Assessing capability and training needs within rural communities*. Richmond: Eastern Kentucky University, Justice and Safety Center.

U.S. Department of Defense. (2011). *Strategy for operating in cyberspace*. Washington, DC: U.S. Department of Defense.

U.S. Department of Homeland Security. (2012). *Emergency services sector cyber risk assessment*.

Washington, DC: U.S. Department of Homeland Security.
U.S. Department of Homeland Security. (2014). *Sector risk snapshots*. Washington, DC: U.S. Department of Homeland Security.
U.S. Department of Homeland Security. (2015a). *Emergency services sector-specific plan: An annex to the NIPP 2013*. Washington, DC: U.S. Department of Homeland Security.
U.S. Department of Homeland Security. (2015b). *Intelligence assessment: Cyber targeting of the U.S. emergency services sector limited, but persistent*. Washington, DC: U.S. Department of Homeland Security, Office of Intelligence Analysis.
U.S. Department of Homeland Security. (2015c). *National preparedness goal* (2nd ed.). Washington, DC: U.S. Department of Homeland Security.
U.S. Fire Administration. (2007). *Mitigation of the rural fire problem: Strategies based on original research and adaptation of existing best practices*. Emmitsburg: U.S. Department of Homeland Security, Federal Emergency Management Agency, U.S. Fire Administration.
U.S. Government Accountability Office. (2008). *Critical infrastructure protection: Further efforts needed to integrate planning for and response to disruptions on converged voice and data networks (GAO-08-607)*. Washington, DC: U.S. Government Accountability Office.
U.S. Government Accountability Office. (2014). *Critical infrastructure protection: More comprehensive planning would enhance the cybersecurity of public safety entities' emerging technology (GAO-14-125)*. Washington, DC: U.S. Government Accountability Office.
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act (Public Law 107-56). 2001, October 26.
Winton, R., & Queally, J. (2016, January 15). FBI is now convinced that couple tried to detonate bomb in San Bernardino terror attack. *The Los Angeles Times*. Retrieved from http://www.latimes.com/local/lanow/la-me-ln-fbi-san-bernardino-bombs-20160115-story.html

Further Reading

Baggett, R., & Simpkins, B. (2018). *Homeland security and critical infrastructure protection* (2nd ed.). Santa Barbra: Praeger Security International.
Lewis, T. (2014). *Critical infrastructure protection in homeland security: Defending a networked nation* (2nd ed.). Hoboken: Wiley.
U.S. Department of Homeland Security. (2013). *NIPP 2013: Partnering for critical infrastructure security and resilience*. Washington, DC: U.S. Department of Homeland Security.

Critical Infrastructure: Government Facilities Sector (GFS)

Ronald L. Martin
Capital Technology University,
Laurel, MD, USA

Keywords
GFS · NRF · NIPP · SSP · NMI · GSA · FISMA · FPS · PBS · WBDG · ISC · NRF · FEMA · CIRC · DoD · CIP · PPD · HSPD · REMS · IHE · Clery · HEA · SSA · UFC

Definition

Security for the Government Facilities Sector (GFS) involves protection of business, judicial, educational, and cultural activities in governmental facilities (Office of Infrastructure Protection 2015).

Introduction

The GFS encompasses federal government facilities that are owned, leased, and operated by the U S government nationally and internationally. Specifically, two US federal organizations – Federal Protective Service (FPS) of the US Department of Homeland Security (DHS) and the General Services Administration (GSA) – oversee its operation (Office of Infrastructure Protection 2015, p. 10). The GFS has two major sub-sectors, including educational facilities (EF) and the national monuments and icons (NMI) (Office of Infrastructure Protection 2015, p. 10). The Department of Education (ED) released the Education Facilities Subsector Snapshot (EDSS) outlining this subsector in 2011, based on Homeland Security Presidential Directive 7 (The White House Office of the Press Secretary 2003). At that time, there were of 18 critical infrastructure sectors (The White House Office of the Press Secretary 2003a). A full description of the 18 critical infrastructure sectors is available on the DHS critical infrastructure resource

center website. Currently, there are 16 critical infrastructures (see all of the Critical Infrastructure entries in this encyclopedia).

The GFS also has five minor sub-sectors: Federal offices and office building complexes; courthouses; archives and libraries; storage and preservation facilities; and embassies, consulates, and border facilities (Office of Infrastructure Protection 2007a, p. 1). The US Marshal Service oversees the federal courthouses. The state, local, territorial, and tribal (SLTT) governments provide protective oversight for nonfederal courthouses. The National Archives and Records (NARA), the Department of Defense (DoD), the Nuclear Regulatory Commission (NRC), and the US Mint which provides specialized oversight to the storage and preservation facilities based on the type of material stored or preserved. And finally, the US Department of State (DOS) and the customs and border patrol of DHS protect embassies, consulates, and border facilities protective measures. Information regarding the minor support agency responsibilities is available on the Homeland Security Digital Library.org website. This entry will describe the GFS sector's vision and goals, assets, and sub-sectors.

GFS Sector Vision and Goals

Chapter three of the 2015 GFS SSP outlines the sector's vision, mission, goals, and priorities (Office of Infrastructure Protection 2015). The SSP vision statement provides a balanced management of sector risks. This risk protocol would allow the government functions to operate without disruption (Office of Infrastructure Protection 2015, Chapter 3, p. 14). The necessary process used to assess risk in the GFS SSP 2015 is important because the 2015 GFS SSP mission is to reduce vulnerabilities while facilitating the resilience and continuity of our nation's operations (Cybersecurity & Infrastructure Security Agency/CISA 2013, p. 14).

In the 2015 GFS SSP, there are five goals with corresponding objectives. The first goal is to implement a facility risk management program. This goal identifies an inventory of worldwide facilities. This inventory assists with the development of a comprehensive risk assessment program. The purpose of this assessment is to develop and promote effective protective measures and strategies. Implementation of the Federal Information Security Management Act of 2002 (The Federal Information Security Management Act (FISMA) of 2002) and the National Institute of Standards and Technology (NIST) cybersecurity programs is essential for the stakeholders to adapt and follow, to perform gap analysis and report findings via a National Annual Report to DHS, and to develop best practice guidance of countermeasures (Office of Infrastructure Protection 2015, Chap. 3, p. 14).

It is crucial to briefly explain the importance of this goal to support the NIPP risk management framework. Central to the NIPP risk management framework is the risk assessment process that incorporates three factors: threat, consequence, and vulnerability. To appreciate these elements, organization should combine the three factors into an equation. Risk equals the combination of threat plus vulnerability plus consequence (or impact). Risk assessments are used to provide reliable and comprehensive data so that security partners can make informed decisions about which risk mitigation measures to implement. In some cases, security partners design risk assessment processes, procedures, methodologies, and tools to meet the specific needs of the facilities they own and operate (Cybersecurity & Infrastructure Security Agency/CISA 2013, p. 17).

The second goal is to create and organize partnerships. There are four objectives associated with this goal. This objective is share information about threats and hazards to facilities internationally as well as domestically; build sector partnerships to implement protection and resilience programs; support continuity programs that protect government operations; and share lessons learned along with any best practices (Office of Infrastructure Protection 2015, Chap. 3, p. 14). GFS security partners include those federal, state, territorial, local, or tribal entities that share in the responsibility for protecting government facilities and their associated elements. Within these sometimes large and complex government entities, security partners represent a wide variety

of facility components that contribute to enhance protection of every facility. Some GFS security partners have different responsibilities, functionality, or expertise based on existing authorities and associated roles. State, local, and tribal governments have the responsibility to implement the homeland security mission, to protect public safety and welfare, and to ensure the provision of essential services to communities and industries within their jurisdictions.

The third goal is to integrate government facility protection with the DHS mission. The supporting objectives are to link the NIPP to the initiatives promoted by the Federal Emergency Management Agency (FEMA). This objective links the NIPP to the National Response Framework (NRF). The importance of the NIPP to NRF alignment is described in the following quote: "The NRF is a guide to how the Nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System (NIMS) to align key roles and responsibilities across the Nation" (FEMA 2016, p. i). The next objective aligned with this goal is to enhance planning and protective measures to align the GFS sector with the National Terrorism Advisory System (NTAS), the Continuity of Government Readiness Conditions (COGCON) system, and the Homeland Security Information Network (HSIN). These key alignments provide the structure needed to alert GFS stakeholders of impending threats, preventative measures, lessons learned, and mitigation best practices. The final objective of this goal is to implement incident management activities (Office of Infrastructure Protection 2015, Chap. 3, p. 15).

The fourth goal is to promote enhanced capabilities of the GFS. "The four objectives that support this goal are to support awareness and understanding of the risks to the GFS are To improve cyber and physical resilience through research and development; Continually develop a GFS SSP to further align with the NIPP; And to promote Executive Order 13636 directed programs of the NIST Cybersecurity Framework and the DHS Critical Infrastructure Cyber Community C^3 (C-Cube) Voluntary Program (Office of Infrastructure Protection 2015, Chap. 3, p. 15)." This GFS goal includes more than just facilities. It also includes physical assets, cyberinfrastructure, positions, and functions that can be essential to the operation of GFS.

The final GFS goal is to maximize and economize the use of resources for GFS protection. The three objectives are to determine GFS priorities and requirements for GFS protection, to enable or facilitate protection for those GFS facilities which are deemed nationally critical, and to outline and decrement countermeasures and mitigation strategies (Office of Infrastructure Protection 2015, Chap. 3, p. 15). A risk assessment is used to provide reliable and comprehensive data to inform risk mitigation decisions. FEMA in 2005 published "Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings" It provides a generic roadmap to basic risk assessment and mitigation methodology (FEMA 452 2005)."

The five sector goals use the goals of the NIPP 2013 and the joint national priorities (JNP). The JNP priorities are risk management, partnerships, capabilities, security, and resilience (Office of Infrastructure Protection 2015). The critical purpose of prioritization is to assist with decrementing resource allocation decisions. GFS stakeholders must determine where protection programs are instituted, the appropriate level of investment in these programs, and which protective measures offer the highest return on investment. Because resources for GFS protection are limited, risk analysis based on practical information must be required before the implementation of sound priorities (Office of Infrastructure Protection 2015, p. 31).

Government Facilities Sector Assets

It is important to outline the diversity of GFS assets. The primary area of the sector is approximately 9000 US federal government facilities encompassing an excess of "3 billion square feet of space and 650 million acres of land" (CIRC 2003a). PBS (2017) manages more than 370 million square feet of workspace in over 8,600 facilities. "The Department of Defense is still one of the Federal government's larger holders of real estate managing a global real property

portfolio that consists of nearly 562,000 facilities (buildings, structures, and linear structures), located on over 4,800 sites worldwide and covering over 24.9 million acres (DoD Base Structure Report FY 2015 Baseline 2016, p. 2)." These numbers do not include the Department of Defense bases, installations, and facilities.

To demonstrate how difficult it is to protect the GFS, consider that before the Interagency Security Committee (ISC) was established under Executive Order 12977 by Clinton, there were no minimal physical security standards for nonmilitary facilities. It was the absence of rigid standards that allowed a 1995 domestic attack on the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, resulting in 168 deaths.

Since 1995, The ISC published policies, standards, and best practices for stakeholders of nonmilitary facilities to follow. In 2003, President Bush, G. W. issued Executive Order 13286. This order transferred the ISC from GSA to DHS (EO 13286 2003). Working with the FPS and the security stakeholders of the federal executive agencies, the ISC provides governance to the GFS. The preponderance of the 2018 standards and guidelines are exempt from public release under the Freedom of Information Act (5 U. S. C. 552). Organizations requiring access to these documents can request them from DHS.

The guidelines focus on the physical security aspects of protection. The ISC has a convergence subcommittee. This subcommittee develops mechanisms to support federal agencies' integration of information management controls with security programs. The Internet of things (IoT) has over the years gained importance to the resilience of our infrastructure (see IoT in this encyclopedia). The resulting threats to physical and cyber systems become an increasing priority for the new threats that will adversely impact the GFS facilities (National Institute of Standards and Technology Interagency 8228 2019, p. iv).

The current devices are the result from the convergence of physical security systems operating on information technology (IT), and operational technology (OT) environments present unique security challenges (NISTIR 8228 2019, p. 5). The IT environment is "...a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information..." (OMB Circular A-130). The OT environment for this discussion is "...any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve the desired result..." (NCCIC 2019, p. 4).

The importance of the convergence subcommittee is to provide a nexus between physical and cybersecurity across these environments. The concept of this subcommittee is to identify issues and challenges agencies may have with security programs and work in collaboration with NIST to integrate physical and cybersecurity management controls. In 2012, the DOC advocated for the use of DHS security standards and risk management applications for all off-installation leased space managed by DoD and all DoD occupied spaced in buildings owned or operated by the US General Services Administration (GSA) (Applied Research Associates Inc 2016).

The role of the ISC is to assist the federal stakeholder in the protection of the facilities within their purview. The ISC centralizes the review of risk management, emergency response, business continuity, physical, logical, and personnel security systems to provide standards and best practices, which will assist agencies in improving their protection of assets and at the same time ensure efficiency. In 2015, the ISC advocated converging traditional security and information technology disciplines in a coordinated effort to secure GFS assets (ISC-CVS 2015).

GFS Sub-sectors

PPD-21 required that the education facilities and the national monuments and icons sectors are within the purview of the GFS (PPD-21 2003). The Office of Safe and Drug-Free Schools (OSDFS) an organization of the US Department of Education (ED) serves as the SSA for the education facilities sector (EFS). The US Department of the Interior (DOI), as the NMI Sector-Specific Agency (SSA), liaises with the DHS Science and Technology Directorate and the Executive Office of the President's Office of Science and Technology Policy (US Department of the Interior 2010, p. 3).

Education Sub-sector

In 2010, an SSP was released by the education facilities (US Department of the Interior 2010 cover). "The EFS covers all public, private, and proprietary education facilities (US Department of Education 2011, p. 1)." These facilities have two distinct institutional types. These types are prekindergarten (PreK) through 12th grade (PreK–12) and higher education campuses. A key ED organization is readiness and emergency for school (REMS) technical assistance center. An essential function of REMS is to facilitate grants and provide safe schools and emergency preparedness programs to the education community.

As mandated by the NIPP of 2009 and the GFS SSP of 2010, the EFS SSP aligns its planned initiatives with the GFS guidance (US Department of Education 2010 EXSUM). This alignment is within the primary sub-sector goal to continue sector progress in emergency management. This progress includes emergency preparedness for schools and higher education. OSDFS facilitate this progress by providing grants and emergency management training (e.g., prevention, mitigation, response, recovery) for schools and universities (US Department of Education 2010, p. 13). It is through this vision statement the EFS can universally support the diversity of the sector's facilities. In short, the sector's value proposition to its stakeholders is "to encourage a resilience approach to emergency management (US Department of Education 2010, p. 14)."

A deliverable of this office's effort was the preparation of the guide for developing high-quality emergency operation plans for institutions of higher education that was prepared for the US Department of Education under Contract Number EDESE12O0036 with Synergy Enterprises, Inc. The EFS OSDFC works closely with DHS and other federal agencies to address protection efforts. OSDFC also coordinates with national interagency collaborations and SLTT governments and private organizations (US Department of Education 2011, p. 2). One federal interagency collaboration was the 2013 release of the guide for developing high-quality emergency operation plans for institutions of higher education. This institution of higher education (IHEs) guide was created through the cooperative efforts of multiple US government sectors (IHE 2013).

An ancillary initiative was the enactment of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (**20 U.S. C. § 1092 (f)). The Clery Center was** founded in 1987 by Howard and Connie Clery following the murder of their 19-year-old daughter, Jeanne, in her dorm (McCallion 2014, p 1)**.** The ED 2016 Edition of the handbook for campus safety and security reporting describes the Clery Act (ED handbook 2016). Numerous laws predicated the Clery Act. The *Higher Education Act of 1965 (HEA) required all postsecondary institutions participating in HEA's Title IV student financial assistance programs to disclose campus crime statistics and security information* (ED handbook 2016, p. 1-1).

The Clery Act amends the requirements of the HEA (Clery handbook 2016, pp. 1-1 to 1-3). Institutions of higher learning except for distant education and foreign institutions must comply with the disclosure requirements of the act (ED handbook 2016, pp. 1-3 to 1-4). "The Clery Act describes that every institution must meet crime statistics and security-related policy. Clery Act requires crime logs for institutions that have a campus police or security departments. HEA requires missing student notification and fire safety requirements for institutions that have at least one on-campus student housing facility (ED handbook 2016, pp. 1-3 to 1-4)." To ensure institutions have the requisite information to perform a risk assessment of the campus, the Clery Act requirements of determining the institution's geography and collecting statistics (ED handbook 2016, pp. 2-1 to 4-12) will assist the institution with applying the NIPP and GFS risk management framework (Cybersecurity & Infrastructure Security Agency/CISA 2013, p. 15) (Office of Infrastructure Protection 2015, p. 17).

National Monuments and Icons Sub-sector

In 2007, DOI released the NMI SSP to ensure that the NMI facilities of other federal agencies and SLTT governments would be aligned and within the purview of GFS and NMI sectors. Three common characteristics define the sector's assets. First, they are a monument, physical structure, or an object. The facilities must represent our nation's heritage, traditions, or values. The final

characteristic is the facility's purpose of memorializing our nation's heritage, traditions, or values (Office of Infrastructure Protection 2007a, 2007b, p. 1). In addition to these three common characteristics of NMI, another factor characterization is that these facilities are open to the public with the minimum of ingress and egress controls, during their hours of operation (Office of Infrastructure Protection 2007a, 2007b, p. 2). Throughout the NMI SSP, the facilities and infrastructure defined as critical infrastructure and key resources or CI/KR. These designations were consistent with the NIPP 2006. This terminology came from homeland security presidential directive-7 (Critical Infrastructure Research Center 2003a, p. 1).

The NMI SSA has a group of authorities that supplement the protection efforts of major federal law enforcement organizations, like the Federal Bureau of Investigation and the Secret Service (US Department of the Interior 2007, p. 56). DOI over the years was given certain legislative authorities to support the agency's protection efforts. A snapshot of some of these authorities is the "Antiquities Act of 1906: Congress passed the Antiquities Act of 1906. This act authorized the President to declare by public proclamation (as national monuments) historic landmarks, historic and prehistoric structures, and other objects of historic or scientific interest" (16 U.S.C. 431).

In 1916, Congress created the National Park Service (NPS) within DOI through an Organic Act for the purpose of preserving specific areas, particularly from development. The General Authorities Act of 1970 (Public Law 91-383, as amended by Public Law 94-458) gave the DOI secretary to designate certain employees of the department as well as officers and employees to act as special policemen within the areas of the NPS. The National Historic Sites Act of 1935 declared as a national policy to preserve for public use historic sites, buildings, and objects of national significance for the inspiration and benefit of the people of the United States. In 40 U.S.C. 6301-6307 provided the Smithsonian Institution's Office of Protection Services the authority to police the buildings and grounds of the Smithsonian Institution (US Department of the Interior 2007, pp. 55–56). The previous listing is a sampling of the authorities given to the DOI. It does provide an abbreviated review of how the SSA provides protection oversight of the sector.

GFS Minor Sub-sectors

Categorization of Facilities and Associated Elements. The minor sub-sectors of the GFS are personnel centric, service-oriented facilities, research and development facilities, storage and preservation facilities, military installations, and space exploration facilities, along with government sensor and monitoring systems (McCarthy 2007 volume 6 number 1). In general, the GFS categorization denotes two distinct types of facilities. The personnel-centric facilities are locations where government personnel work and conduct the business of the government. They have limited public access and typically do not experience large numbers of visitors (Office of Infrastructure Protection 2007e, p. 1). The second type is service-oriented facilities; these facilities provide services to the government and the general public. They experience large numbers of citizens. These facilities typically contain the technical equipment necessary to carry out and deliver government services (Office of Infrastructure Protection 2007f, p. 1).

Federal offices and office building complexes are "government facilities that are categorized based on the main function or purpose of the building or its primary use. Personnel-centric facilities house government personnel in the course of official business or personal pursuits (Office of Infrastructure Protection 2007e, p. 1)." Additionally, data centers, as well as federal SLTT office buildings, are included within this sub-sector.

The courthouse is a minor subsector of the GFS. The subsector includes facilities owned, operated, and leased by all levels of government. The federal court system (FCS) consists of 94 district courts, 13 circuit courts throughout the country, and 1 supreme court located in Washington D. C. These courts may represent two or more facilities (Office of the United States Attorneys 2019). In addition to the federal court system, state, local, tribal, and territorial (SLTT) jurisdictions have the responsibility to enforce state and local laws and ordinances. The scope of these facilities includes all 50 states, 3,043 counties, 19, 372 municipal, and 16, 629 township jurisdictional courts.

The federal court's system security and protection is the responsibility of the US Marshal Service. The Marshal Service established in 1789 (US Marshals Service 2019). The SLTT governments have the responsibility for protecting and securing court fall to the cognizant law enforcement jurisdiction. As such, the NMI 2007 conformed to the NIPP risk management framework of 2006 (Office of Infrastructure Protection 2006, p. 4). This version of the NIPP showed six elements of this framework. These elements are "set security goals; identify assets, systems, networks, and functions; Assess risks; prioritize; implement protective programs; And measure effectiveness (Office of Infrastructure Protection 2006, p. 4)." With the release of the NIPP of 2013, the chevron element of prioritizing was removed (Office of Infrastructure Protection 2013, p. 15). However, within the 2013, version of the NIPP prioritization is included within the measure effectiveness chevron. Realigning the risk management framework assures the identification of high-level outputs or outcomes associated with the national goals and priorities (Office of Infrastructure Protection 2013, p. 20).

Storage and preservation facilities are a complex minor subsector of GFS. These facilities include centers that store records and materials that require permanent protection for historical and lifetime storage, upkeep, and preservation (Office of Infrastructure Protection 2007f, p. 1). The National Archives and Records Administration (NARA) is responsible for the national personnel records and the federal record centers (Office of Infrastructure Protection 2007d, p. 1). The subsector is also responsible for oversight of specialized storage facilities housing precious metal and currency, weapons and ammunition and special nuclear materials, and waste (Office of Infrastructure Protection 2007g, p. 1). The US Mint, the Department of Defense, and the Nuclear Regulatory Agency provide direct oversight over those areas within their area of responsibility.

An important function of NARA is to provide direct oversight of archives and libraries. The National Archives is the repository of US documents (Office of Infrastructure Protection 2007d, p. 1). The sector through NARA has oversight for presidential and federal libraries. The sector includes libraries associated with education facilities. The ED SSP will have direct oversight of college and university libraries by the requirements of the Clery Act. Public libraries would be the responsibility of SLTT governments (Office of Infrastructure Protection 2007d, p. 2).

The US Department of State (DOS) and the customs and border patrol of DHS oversee embassies, consulates, and border facilities measures. The US government has diplomatic relations with about 180 countries. A US mission manages American diplomatic and consular activities (Office of Infrastructure Protection 2007c, p. 1). The Bureau of Diplomatic Security (DS) personnel – who include special agents, engineers, diplomatic couriers, civil service specialists, and contractors – work together as a team to ensure that the state department can carry out its foreign policy missions safely and securely. In the USA, the Bureau protects the Secretary of State, the US Ambassador to the United Nations, and foreign dignitaries below the head-of-state level who visit the United States. DS develops and implements security programs to protect the more than 100 domestic state department facilities as well as the residence of the secretary of state. Lastly, border stations are a "land port of entry" that provide controlled egress from the United States for persons and materials. A border station houses US Customs and Border Protection and other Federal Inspection Agencies responsible for the enforcement of federal laws about entry into or departure from the USA (Office of Infrastructure Protection 2007, p. 2).

Conclusion

Providing services to the citizens of the USA is a core function of the GFS. The sector's complexity requires a wide range of coordination with public and private stakeholders. The sector's facilities educate our nation's population, provide and house facilities that conduct administration of justice activities, and preserve the heritage of our nation. The services provided by the GFS are crucial to the protection and resilience of our nation. One major private sector contribution to this collaboration is the Clery Center. The Clery Center's operation is indicative of the nonprofit and not-for-profit organizations that are crucial to

the GFS accomplishing its vision and goals. The federal sector element relies on the cooperation of SLTT governments. The release of the 2015 GFS SSP enhanced the coordination between all GFS stakeholders. Interested personnel and organizations can now use the GFS SSP freely to give the sector community the governance needed to enhance protective and resilience thinking.

Cross-References

- ▶ Critical Infrastructure: Commercial Facilities Sector
- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Emergency Services Sector
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector

References

Applied Research Associates, Inc. (2016). *Whole Building Design Guide (WBDG) Unified Facility Code (UFC)/ Interagency Security Committee (ISC) UFC/ISC Security Criteria Overview and Comparison*. Washington, DC: National Institute of Building Sciences. http://www.wbdg.org/resources/ufc-isc-security-criteria-overview-and-comparison.

Bush, G. W. (2003a). *Presidential Policy Directive-7: Critical infrastructure identification, prioritization, and protection*. Washington, DC: The White House: Office of the Press Secretary. https://www.dhs.gov/homeland-security-presidential-directive-7.

Bush, G. (2003b). *Executive Order 13286: Amendment of executive orders, and other actions, in connection with the transfer of certain functions to the Secretary of Homeland Security*. Washington, DC: Office of the Federal Register. https://www.hsdl.org/?view&did=1361.

Clinton, B. (1995). *Executive Order (EO) 12977: Interagency Security Committee (ISC) United States*. Washington, DC: Office of the Federal Register. https://www.hsdl.org/?view&did=439290.

Critical Infrastructure Resource Center. (2003a). *Summary of Critical infrastructure protection sectors circa 2003*. Washington, DC: US Department of Homeland Security. http://www.humtech.com/fema/CIKR_RC/sectorMenu.htm.

Critical Infrastructure Resource Center. (2003b). *Summary of government facilities sector circa 2003*. Washington, DC: US Department of Homeland Security. http://www.humtech.com/fema/CIKR_RC/govt Fac1.htm.

Cybersecurity and Infrastructure Security Agency (CISA). (2007). *Government facilities sector: Embassies, consulates, and border facilities. (Publication no. 775444)*. Washington, DC: US Department of Homeland Security. http://www.hsdl.org/?view&did=775444.

Cybersecurity and Infrastructure Security Agency (CISA). (2013). https://www.hsdl.org/?view&did=733614

Cybersecurity and Infrastructure Security Agency (CISA). (2015). *Critical infrastructure sectors: Government facilities sector: An annex to the NIPP 2013*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf.

Dept of Homeland Security. (2016). National response framework, 3rd ed. https://www.ready.gov/sites/default/files/2019-06/national_response_framework.pdf.

Fautsko, T. (2013). *Status of court security in State Courts*. Williamsburg: National Center for State Courts. https://ncsc.contentdm.oclc.org/digital/collection/facilities/id/184.

Federal Emergency Management Agency (FEMA). (2005). *Risk assessment a how-to guide to mitigate potential terrorist attacks against buildings (FEMA Publication 452)*. Washington, DC: US Department of Homeland Security. https://www.fema.gov/media-library-data/20130726-1524-20490-7395/fema452_01_05.pdf.

Interagency Security Committee (ISC). (2012). *Facility Security Committees*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/isc-facility-security-committees-standard-january-2012-2nd-edition.pdf.

Interagency Security Committee (ISC). (2015a). *Securing government assets through combined traditional security and information technology: An Interagency Security Committee white paper*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/ISC-CVS-White-Paper-2015-508.pdf.

Interagency Security Committee (ISC). (2015b). *Facility security plan: An Interagency Security Committee guide*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/ISC-Facility-Security-Plan-Guide-2015-508.pdf.

Interagency Security Committee (ISC). (2016). *The risk management process for Federal facilities*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf.

Interagency Security Committee (ISC-CVS). (2015). *Securing government assets through combined traditional security and information technology*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/ISC-CVS-White-Paper-2015-508.pdf.

McCallion, G. (2014) *History of the Clery Act: Fact sheet Library of Congress*. Washington, DC: Congressional Research Service (CRS). http://clery.clerycenter.org/wp-content/uploads/2015/09/nps69-111214-12-3-2.pdf

McCarthy, J. (2007). *Inside the Government Facilities Sector. The CIP report July 2007 volume 6 number 1*. Fairfax: George Mason University, School of Law. https://cip.gmu.edu/wp-content/uploads/2013/06/60_The-CIP-Report-July-2007_GovernmentFacilitiesSector.pdf.

National Cybersecurity & Communications Integration Center (NCCIC). (2019). *Introduction to industrial control systems cybersecurity (101) training course manual*. Washington, DC: US Department of Homeland Security.

National Institute of Standards and Technology Interagency. (2019). Considerations for managing internet of things (IoT) cybersecurity and privacy risks internal report 8228. US Department of Commerce. Washington, DC. https://doi.org/10.6028/NIST.IR.8228

Obama, B. (2013a). Executive Order 13636: Improving critical infrastructure cybersecurity. *Federal Register, 78*(33), 11739. Executive Office of the President of the United States, Washington, DC. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.4938&rep=rep1&type=pdf

Obama, B. (2013b). *Presidential Policy Directive-21: Critical infrastructure protection and resilience*. Washington, DC: The White House. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Office of Cyber and Infrastructure Analysis, (OCIA). (2014). *Sector risk snapshots (Publication no. 754033)*. Washington, DC: Department of Homeland Security. https://hsdl.org/?wiew&did=754033.

Office of Infrastructure Protection. (2006). *National Infrastructure Protection Plan*. Washington, DC: US Department of Homeland Security. https://fas.org/irp/agency/dhs/nipp.pdf.

Office of Infrastructure Protection. (2007). *National Monuments and Icons Sector Facts*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-national-monuments-and-icons-snapshot-2011.pdf

Office of Infrastructure Protection. (2007a). *Government facilities sector: Categorization of facilities and associated elements*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=775153.

Office of Infrastructure Protection. (2007b). *Government facilities sector: Courthouses*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=775370.

Office of Infrastructure Protection. (2007c). *Government facilities sector: Embassies, consulates, and border facilities*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=775444.

Office of Infrastructure Protection. (2007d). *Government facilities sector: Archives and libraries*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=775002.

Office of Infrastructure Protection. (2007e). *Government facilities sector: Offices and office building complexes*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=775508.

Office of Infrastructure Protection. (2007f). *Government facilities sector: Storage and preservation facilities*. Washington, DC: US Department of Homeland Security.

Office of Infrastructure Protection. (2007g). *Government facilities sector: Security partner roles and responsibilities*. Washington, DC: US Department of Homeland Security.

Office of Management and Budget. (2016). Managing Information as a Strategic Resource OMB Circular No. A–130. *Federal Register, 81*(145). Executive Office of the President. Washington, DC. https://www.govinfo.gov/content/pkg/FR-2016-07-28/pdf/2016-17872.pdf.

Office of Safe and Drug-Free Schools (OSDFS). (2010). *Education facilities sector-specific plan an annex to the government facilities sector-specific plan*. Washington, DC: US Department of Education. https://www.dhs.gov/xlibrary/assets/nipp-ssp-education-facilities-2010.pdf.

Office of Safe and Drug-Free Schools (OSDFS). (2011). *National Infrastructure Protection Plan Education Facilities Subsector-snapshot*. Washington, DC: US Department of Education. https://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-education-facilities-snapshot-2011.pdf.

Office of the Secretary of Defense. (2016). *The Base Structure Report (BSR) – FY 2015 baseline*. Arlington: Department of Defense. http://www.kritisches-netzwerk.de/sites/default/files/us_department_of_defense_-_base_structure_report_fiscal_year_2015_baseline_-_as_of_30_sept_2014_-_a_summary_of_the_real_property_inventory_-_206_pages.pdf.

Office of the United States Attorneys. (2019). *Introduction to the federal court system*. Washington, DC: United States Department of Justice. https://www.justice.gov/usao/justice-101/federal-courts.

Office of Infrastructure Protection. (2015). *Government Facilities Sector: Sector Specific Plan*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf

Office of Infrastructure Protection. (2013). National Infrastructure Protection Plan. (2013). *Partnering for critical infrastructure protection and resilience*. Washington, DC: Department of Homeland Security. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-andresilience

Public Building Service (PBS). (2017). *Public building service: An overview*. Washington, DC: US General Services Administration. https://interact.gsa.gov/sites/default/files/PSHC%20SYMP_PBS_Overview_presentation_CLP.pdf.

The Federal Information Security Management Act (FISMA) of 2002. Public Law 107–347 116 STAT. 2899. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

United States Park Police (USPP). (2011). *National Infrastructure Protection Plan National Monuments and Icons Sector-snapshot*. Washington, DC: US Department of the Interior. https://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-national-monuments-and-icons-snapshot-2011.pdf.

US Department of Education (ED). (2010). *Education facilities sector-specific plan 2010*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=736907.

US Department of Education (ED), Office of Safe and Drug-Free Schools (OSDFS). (2011). *National Infrastructure Protection Plan: Education facilities subsector*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/nppd/nppd-ip-education-facilities-snapshot-2011.pdf.

U.S. Department of Education. (2013). *Guide for developing high-quality emergency operations plans for institutions of higher education*. Washington, DC: Federal Emergency Management Agency. https://www.fema.gov/media-library-data/20130726-1922-25045-3638/rems_ihe_guide.pdf

US Department of the Interior. (2007). *National Monuments & Icons Critical Infrastructure and Key Resources Sector-specific plan as input to the National Infrastructure Protection Plan*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=232381.

US Department of the Interior. (2010). *National Monuments and Icons Sector-Specific Plan, an annex to the National Infrastructure Protection Plan 2010. (Publication no. 691263)*. Washington, DC: US Department of Homeland Security. https://www.hsdl.org/?view&did=691263.

US Election Assistance Commission. (2019). Elections critical infrastructure. https://www.eac.gov/election-officials/elections-critical-infrastructure/

US Marshals Service. (2019). *Fact sheet: Judicial security*. Washington, DC: United States Department of Justice. https://www.usmarshals.gov/duties/factsheets/judicial_sec.pdf.

Further Reading

Federal Emergency Management Agency. (2008). *Emergency support functions annexes: Introduction*. Washington, DC: US Department of Homeland Security. https://www.fema.gov/pdf/emergency/nrf/nrf-esf-intro.pdf.

Interagency Security Committee. (2015). *Planning and response to an active shooter: An Interagency Security Committee policy and best practices guide*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/isc-planning-response-active-shooter-guide-non-fouo-nov-2015-508.pdf.

Interagency Security Committee. (2019). *Interagency Security Committee violence in the federal workplace guide (July 2019/2nd Edition) with appendices*. Washington, DC: US Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/isc_workplace_violence_guide_-_2019_0.pdf and https://www.dhs.gov/sites/default/files/publications/isc_workplace_violence_appendices_-_2019_0.pdf.

Public Building Service. (2012). *PBS leasing desk guide*. Washington, DC: General Services Administration. https://www.gsa.gov/cdnstatic/LDG-Chapter19_9-28-12_final_508.pdf.

Critical Infrastructure: Nuclear Reactors, Materials, and Waste Sector

Adam D. Williams
Center for Global Security and Cooperation, Sandia National Laboratories, Albuquerque, NM, USA

Keywords
Reactor security · Nuclear materials

Definition

Nuclear reactors provide several key societal benefits – including electricity generation and industrial/medical isotope production – that need to be protected against malicious activities.

SAND2018-9356J. Sandia National Laboratories is a multimission laboratory managed and operated by the National Technology & Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525

Introduction

Nuclear technologies provide a range of benefits to the society. These benefits include reduced carbon emission electricity production, seawater desalination, generating radionuclides to serve various medical needs (including cancer treatments), and advanced technological development. As such, these activities and facilities are assessed by the Department of Homeland Security (DHS) to be critical because:

> a significant incident or failure. . .would likely result in extremely high economic costs, major onsite and/or offsite property damage, and evacuations. . .[as well as] long-term cleanup costs and economic damage to the local region. (DHS 2015, p. 9)

Therefore, to ensure these benefits are realized, facilities hosting these technologies fall under the purview of the US Department of Homeland Security's *Nuclear Reactors, Materials, and Waste Sector*. Given that the natural and physical characteristics of nuclear materials pose unique – and potentially catastrophic – consequences, related security and emergency management responsibilities must mitigate such current threats as expanding terrorist capabilities, increasingly sophistical cyber actions, aging equipment (including power grids), and supply chain challenges.

The rest of this paper describes efforts at such protection by focusing on nuclear reactors as a use case. After briefly introducing the need for reactor security, unique challenges, key security concepts, and common themes between different approaches to reactor security are discussed. These challenges, concepts, and common themes are reflective of the larger *Nuclear Reactors, Materials, and Waste Sector* and aid in protecting this critical infrastructure.

What and Why of Reactor Security

Nuclear reactors generate these aforementioned benefits by using the energy released during the rapid and exponentially increasing collisions of atomic and subatomic particles known as nuclear fission. The process of fission has two major products. The first is a large amount of thermal energy, or heat – captured from the fission of nuclear materials (Nuclear materials is a term designated for elements capable of sustaining fission in a controlled chain reaction and is commonly known to consist of uranium, plutonium, and thorium) – that is converted into electricity or used in desalination. The second product results from the change in the atomic structure of the materials that undergo fission – which is how the various radionuclides that support medical and industrial needs are generated.

Two major categories of nuclear reactors manipulate nuclear fission to different ends. The first is known as *power reactors* and is primarily used to generate electricity or for desalination for societal consumption. For example, the United States has 99 operating nuclear power reactors that account for approximately 20% of its domestic electricity production (DHS 2015). Similarly, the International Atomic Energy Agency's (IAEA) Power Reactor Information System (PRIS) reports 450 nuclear power reactors internationally that account for approximately 11% of global electricity production, with the highest nuclear energy-based electricity production of over 70% in France (International Atomic Energy Agency 2018b). Through PRIS, the IAEA also reports more than 50 new nuclear power reactors in various stages of consideration or under construction – including in Belarus, China, Turkey, Russia, and the United Arab Emirates (International Atomic Energy Agency 2018b).

The second major category consists of research reactors that are smaller, produce less thermal power, and are used for a variety of purposes. According to the IAEA's Research Reactor Database (RRDB), there are 225 research reactors worldwide, including 31 in the United States. Research reactors can be used for exploring new nuclear fuel cycles, neutron activation analysis, and educational purposes (International Atomic Energy Agency 2018a). These reactors are also commonly used to generate radioisotopes used in medical

procedures, to include the need for strontium-89, palladium-107, iridium-192, and iodine-125 (or 131) in cancer treatments. In addition, these reactors produce the molybdenum-99 used in medical imaging devices. Research reactors are also used to generate isotopes for industrial uses, to include (but not limited to) iridium-192 and selenium-75 used in industrial radiography, as well as americium-241 for well-logging and commercial/residential smoke detectors. Research reactors are less technically complex than power reactors, require significantly less fuel to operate, use higher-enriched fuel than power reactors, and their designs avoid the high temperatures and pressures of electricity-generating reactors. Research reactors can exist in wide-ranging operational environments, including universities, medical facilities, and commercial campuses around the world (National Academy of Sciences 2016).

To ensure these societal benefits are enjoyed, the efforts to make nuclear reactors, materials, and waste secure and resilient must protect against "[any] deliberate act against a [nuclear reactor] that could directly or indirectly endanger public health and safety through exposure to radiation" (Holt and Andrews 2014). Such deliberate activities include sabotage (either by directly or indirectly adding energy to cause a radiological release), theft (removing materials to use in an offsite radiological release), and unanticipated reactor transients (causing operations to slow/stop and resulting in unacceptable consequences such as loss of profit or reputation) (Please see chapter ▶ "Insider Threat," for further discussion.).

Examples of malicious acts against nuclear facilities include:

- **2012**: Activists entered two Swedish nuclear power plants without being stopped by guards, and four of them hid overnight on a reactor building roof (MacFarlene 2016).
- **2014**: French nuclear power plants were plagued by unexplained drone overflights that challenged existing reactors security measures (Solodov et al. 2018).
- **2014**: An unidentified adversary tampered with turbine lubricant at the Doel Nuclear Power Station in Belgium causing Unit 4 to shut down for 5 months (MacFarlene 2016).
- **2016**: French investigators discovered video surveillance footage of a Doel Nuclear Power Station official in the home of one of the Paris terror attack suspects (MacFarlene 2016).

Unfortunately, these cases highlight the real threat against nuclear reactors and emphasize the need for protection of these critical pieces of infrastructure. In addition to deliberate terrorist acts, the US Department of Homeland Security has recently identified the following risks related to security of both nuclear reactors and other aspects within the nuclear energy sector, to include (DHS 2015, pp. 9–10):

- Natural disasters and extreme weather
- Structural issues of specialized designs and components
- An aging infrastructure and workforce
- Cyberattacks
- Supply chain disruptions
- Nuclear material diversion or mishandling

To that end, the goal of reactor security is to protect people, infrastructure, and the environment from radiological releases caused by malicious acts. Pointedly, nuclear reactor security should be:

> designed to protect three primary areas of vulnerability: controls on the nuclear chain reaction, cooling systems that prevent hot nuclear fuel from melting even after the chain reaction has stopped, and storage facilities for highly radioactive spent nuclear fuel. (Holt and Andrews 2014, p. 1)

Unique Challenges Facing Nuclear Reactor Security

Yet, the special physical properties of nuclear reactors pose a set of additional – and unique – challenges for security and emergency management efforts. The first unique challenge in securing nuclear reactors is the danger related to radioactive materials (Radioactive materials can consist of several species of the same chemical element with different masses whose nuclei are unstable and dissipate excess energy by

spontaneously emitting radiation in the form of alpha, beta, and gamma rays). To achieve their societal benefit, reactors use a subset of these radioactive materials capable of sustaining chain reactions to harness the energy released by fission. By-products of nuclear fission are atomic fragments with unstable nuclei, which is the physical phenomenon that makes them radioactive. Radioactive materials also carry particular, severe, and psychologically fear-inducing characteristics related to acute (e.g., radiation poisoning) and delayed (e.g., latent cancer) human health effects. Despite the fact that materials used in power reactors is not viable for military use, nuclear materials are often conflated with the danger associated with nuclear weapons. The dangers attributed to radioactive materials – both factual and perceived – create a higher standard for reactor security beyond that traditionally expected for other critical infrastructure.

These radioactive materials also need special handling equipment, rules, and processes to ensure that these materials – and the energy they produce – are used in a controlled manner. One example of special handling equipment are reactor cooling systems that consist of both active (e.g., using energy to dissipate heat in the reactor like forced flow cooling loops in nuclear power plants) and passive (e.g., allowing heat to dispel naturally as with cooling towers) mechanisms. Another example of special handling equipment relates to the need to store the highly radioactive nuclear fuel that has been used in a reactor. So-called spent nuclear fuel (in some arenas, this term is called "used nuclear fuel") is most commonly stored in large pools of water or in large concrete casks. As indicated by Holt and Andrews (2014), in addition to the nuclear reactor itself, another challenge is that each of these pieces of special handling equipment also requires protection from malicious activities.

Nuclear reactors must also safely function in multifaceted operational environments and handle physical environments with extremely high temperatures and pressures. Nuclear reactors must also navigate long operational lifetimes (often 40–60 years for power reactors) with the industrial emphasis on safety, a significant emphasis on production, and where, according to one nuclear security expert, "every dollar that a facility manager spends on protection is a dollar not spent on revenue-generating production" (Bunn 2005). Operations at nuclear reactors must also survive under the scrutiny and influence of fluctuating public opinion over the correct balance between the societal benefits provided and risks (real and perceived) accepted. For power reactors, their infrastructure footprint and larger number of moving parts present a wider range of potential threats, while the large workforce also poses potential conflicts for security-related activities. For research reactors, their smaller infrastructure footprint and smaller number of moving parts present less of a range of potential threats, but their proximity to other operations can result in less control over access to the reactor or its special handling equipment – which represents a special set of potential challenges to reactor security. Each of these unique challenges are dimensions that must be accounted for when protecting nuclear reactors.

Reactor Security: Key Concepts

Despite these threats and challenges, efficient and effective reactor security is based on several key concepts. The first key concept is that reactor security starts with the regulations established at the national level. Most commonly, a designated competent authority drafts such regulations, communicates them to individual facilities, and ensures their enforcement (International Atomic Energy Agency 2017a). Each facility with a nuclear reactor is then responsible for translating these regulations into site-specific policies and procedures that align with its unique operational environment. Consider, for example, regulations and policies that relate to the different security zones within (and around) nuclear reactor facilities. More specifically, in the United States:

> The [nuclear reactor] sites are divided into three zones: an "owner controlled" buffer region, a "protected area," and a "vital area." Access to the protected area is restricted to a portion of plant

> employees and monitored visitors, with stringent access barriers. The vital area is further restricted, with additional barriers and access requirements. (Holt and Andrews 2014, p. 1)

While the national-level competent security authority mandates the existence of these zones, the nuclear reactor facility is responsible to operationalize them with the proper security technologies and procedures. This is an example of the importance of clearly and effectively communicating and implementing the different security-related responsibilities between national-level and facility-level nuclear stakeholders.

The second key concept relates to *preventive measures* to protective nuclear reactor facilities. These measures seek to stop malicious activities to reactor facilities before undesired consequences are experienced. Some preventive measures seek to *detect* malicious activities in order to initiate a mitigation, or response, and can consist of such measures as video cameras, motion sensors, closed-circuit television systems, and human observation. Another type of preventive measure seeks to *delay* malicious activities through the use of physical barriers (e.g., bullet-resistant surfaces within the reactor facility) or administrative controls (e.g., access requirements into the reactor building). Preventive measures also include efforts to increase trustworthiness among facility personnel and can include (but are not limited to) background investigations, highly trained security officers, and programs that incentivize adhering to security procedures (For further discussion on detection, please see chapters ►"Intrusion Detection Systems," ►"Physical Security: Interior Applications," or ►"Physical Security: Video Surveillance, Equipment, and Training".).

Mitigation measures – the third key concept – seek to contain or reduce the severity of undesired consequences resulting from malicious activities. For nuclear reactors, the primary mitigation for suppressing such consequences is the containment structures (meter-thick steel-reinforced concrete) enveloping the reactors. Similarly, reactor facilities have safety systems in place for quickly stopping the nuclear chain reaction occurring in the reactor. In this case, the control room for reactor operations – more specifically, the ability to drop control rods into the reactor or to flood the reactor core – represents another mitigation measure. Additionally, the existence of different "security zones" represents yet another mitigation measure by increasing the distance between the results of a malicious activity against the reactor and subsequent dangers to the public.

Common Themes and Guiding Principles

Despite the lack of global standards (MacFarlane 2016), there are common themes and lessons to be learned from various applications of these key concepts that can serve a strong foundation for reactor security. First, nuclear reactors face a unique set of challenges to effective security above and beyond those traditionally associated with other types of critical infrastructure. Second, effective reactor security is predicated on the combination of strong regulatory standards at the state level, performance requirements established by the competent security authority, and implementation of related technological and procedural measures at the facility level. Third, reactor security must be effectively coordinated across facility operations and properly employed for sustained long-term success.

In addition, strong reactor security can be built using a few long-established guiding principles supported by both international best practices – including from the IAEA's Nuclear Security Series (International Atomic Energy Agency 2017b) and the World Institute for Nuclear Security's Best Practice Guides (2018) – and US-based documents (e.g., US Nuclear Regulatory Commission (2017) and US Department of Homeland Security (2015) regulations and reports). First, the safety principle of *defense-in-depth* describes the benefits of creating multiple, concentric layers of protection measures around nuclear reactors can enhance robustness reliability and resiliency of security performance. Second, the principle of *balanced protection* describes the importance of equivalence between protection

measures that compose a security layer. Moreover, this second principle describes the importance of removing as many "weakest links" as possible – ensuring that similar access controls are in place at the main facility entrance and the loading dock, for example.

Third, the principle of taking a *graded approach* to reactor security describes how the selection and implementation of both technological and administrative protection measures are scaled to align with the operations of the nuclear facility – nuclear power plants need a larger security infrastructure than research reactor facilities, for example. Fourth, the guiding principle for reactor security to be *risk-based* describes how decisions related to the selection and implementation of protection measures are quantitatively mapped to clearly define undesired consequences and the current understanding of potential malicious activities against the facility.

Conclusion

Reactor security is a necessary – albeit complicated and complex – aspect of ensuring that the economic, public health, and societal benefits continue to be enjoyed without significant radiological impact to the environment. The common themes and guiding principles for reactor security discussed above are consistent with the risk mitigation strategies and goals provided in the DHS sector-specific plan (DHS 2015), which include:

- Establishing robust collaboration/communication channels and protocols
- Identifying sector-specific threats and vulnerabilities to enable a risk-informed approach
- Developing programs and measures to cost-effectively reduce physical/cyber risks
- Supporting planning and risk mitigation for coordinated response and rapid recovery
- Promoting continuous learning and adaptation to reduce nuclear risks

Taken together, leveraging these common themes and guiding principles can enable strong and sustainable security and emergency management efforts not just for nuclear reactor facilities but also for the larger set of nuclear-related pieces of critical infrastructure. More specifically, reactor security helps support the DHS nuclear sector vision to "support national security, public health and safety, economic stability by enhancing. . .the security and resilience of the Nuclear Sector in an all-hazards environment" (DHS 2015, p. 30).

Cross-References

- ▶ Insider Threat
- ▶ Intrusion Detection Systems
- ▶ Physical Security: Exterior Application
- ▶ Physical Security: Interior Applications
- ▶ Physical Security: Video Surveillance, Equipment, and Training

References

Bunn, M. (2005). Incentives for nuclear security. In *Proceedings of the 46th annual meeting of the institute of nuclear materials management (INMM)*. Phoenix: INMM.

Holt, M., & Andrews, A. (2014). Nuclear power plant security & vulnerabilities, Congressional Research Service, Report for Congress RL34331.

International Atomic Energy Agency. (2017a). Member States' competent authorities. https://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx.

International Atomic Energy Agency. (2017b). Nuclear security series. https://www.iaea.org/resources/nuclear-security-series.

International Atomic Energy Agency. (2018a). Research reactor database. https://nucleus.iaea.org/RRDB/RR/ReactorSearch.aspx.

International Atomic Energy Agency. (2018b). The database on nuclear power reactors. IAEA's Power Reactor Information System. https://pris.iaea.org/PRIS/home.aspx.

MacFarlane, A. (2016). "How to Protect Nuclear Plants from Terrorists" U.S. News & World Report, April 13. https://www.usnews.com/news/articles/2016-04-13/how-to-protect-nuclear-plants-from-terrorists.

National Academies of Sciences. (2016). Chapter 3: Research reactors and their uses. In *Reducing the use of highly enriched uranium in civilian research reactors*. Washington, DC: The National Academies Press.

Solodov, A.A., Williams, A.D., Al Hanaei, S., and Goddard, B. (2018) Analyzing the threat of unmanned

aerial vehicles (UAV) to nuclear facilities. Security Journal, 31(1), 305-324.
U.S. Department of Homeland Security. (2015). Nuclear reactors, materials, and waste sector-specific plan: An Annex to the NIPP 2013. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf.
U.S. Nuclear Regulatory Commission. (2017). Physical protection. https://www.nrc.gov/security/domestic/phys-protect.html.
World Institute for Nuclear Security. (2018). Category: Best practice Guides. https://www.iaea.org/resources/nuclear-security-series.

Further Reading

Behrens, C., & Holt, M. (2005). Nuclear power plants: Vulnerability to terrorists. Congressional Research Service, Report for Congress RS21131.
International Atomic Energy Agency. (2011). *Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/Revision 5)*. Vienna: International Atomic Energy Agency.
U.S. Code of Federal Regulations. (2017). Part 73 – Physical Protection of Plants and Materials (10 C.F.R. 73).

Critical Infrastructure: Transportation Systems

Richard R. Young[1] and Gary A. Gordon[2]
[1]School of Business Administration, Capital College, The Pennsylvania State University, Middletown, PA, USA
[2]Emergency Management Department, Massachusetts Maritime Academy, Buzzards Bay, MA, USA

Keywords
Security · Resilience · Natural disasters · Manmade disasters · Transportation infrastructure · Transportation modes

Definition

Transportation infrastructure is the collection of rights-of-way, terminals, maintenance support facilities, and communications and control fixed assets necessary for the movement of goods and people from one location to another. Its protection is found in the means of preventing its damage or destruction but also in those activities that mitigate any potential damage in order that the infrastructure be returned to service in the most efficient and effective manner.

Introduction

Protecting transportation infrastructure in the United States requires an understanding of its ownership, the characteristics of each mode, the relevant governing political jurisdictions, and various protective approaches including public policy initiatives. Moreover, there is the realization that the topic of infrastructure is bifurcated into physical and informational categories, again each with particular modal variations and operating characteristics.

Infrastructure ownership can be divided between the public and private sectors; however, because transportation exists as a system, these normally operate in a nearly seamless fashion as both passengers and cargo may traverse both between points of origin and those of destination. Again, because transportation is a system, multiple modes may be utilized as well as multimodal transportation activities and more recently by the long-term growth in intermodal services. Where the matter becomes more complex is with those situations where multiple modes may share the same rights-of-way or facilities or be in close proximity. An example of this within the same mode are where Amtrak, the National Rail Passenger Corporation, shares trackage with Norfolk Southern, a freight railroad operating in the private sector. There are also instances of Amtrak owning tracks that are immediately adjacent to those of CSX, another freight railroad, or light-rail operated by the Port Authority Trans Hudson (PATH) in greater New York/New Jersey (Plant and Young 2007). A most frequently found situation is where highways and railroads operate in close proximity such as with parts of the Interstate 95 corridor.

This entry shall endeavor to address protecting the infrastructure associated with railroads, roads

and highways (aka motor carriage), maritime transport including both inland waterways and open sea, pipeline, and aviation. This is an extensive topic, and the reader is directed to the modal-specific entries found elsewhere in this encyclopedia for in-depth coverage.

Differentiating Links and Nodes

Infrastructure includes terminals and intermodal connections that logisticians term as nodes and rights-of-way connecting those nodes known as links but also maintenance facilities, administration buildings, classification yards, and communications towers for traffic control. As further detail, terminals need to be thought of as those points where transportation services are accessed. Rights-of-way need to be built over a range of geographies; hence, they require bridges, tunnels, culverts, and dredged channels. Rights-of-way exist as expanses of land for carrying rail lines and roadways but also as sea-lanes, air corridors, and subterranean routes carrying pipelines (Plant and Young 2007; Talarico et al. 2016).

There is a range of information-related infrastructure components that continue to grow as technology advances. In earlier times, these marked safe routes of travel, the most obvious of which would be lighthouses, but were later joined by buoys and even later by traffic lights and railway signals. Aviation is now controlled by air traffic control systems, and all forms of information-related infrastructure have become digital combining robust communications capabilities as well (Edwards and Goodrich 2013).

Transportation as a Derived Demand Activity

With few exceptions, the demand for transportation within any mode is derived from the demand for the underlying goods or for the need of people to be transported from a place of supply to one of need. As the population migrates and available products proliferate, the demand patterns also shift. Existing infrastructure may need to be expanded or even new infrastructure built. Moreover, some existing infrastructure may need to be de-emphasized. However, a hallmark of transportation infrastructure is that it may see service for a period spanning a century or more; hence, the priorities assigned to it at one point may no longer be relevant at a later date (Garrison and Levinson 2014).

Most people do not think about transportation infrastructure despite their being dependent upon the service it enables. While it is "just there," it is also expected to be "just there" whenever someone needs to travel from point A to point B or when they have some form of material or service need in everyday life. This is to say that transportation infrastructure is largely invisible until it represents an inconvenience.

Unimodal and Multimodal Considerations

Various modes have different requirements for infrastructure but also differing ownership and maintenance needs. For example, airlines require significant investment in terminals and air traffic control systems; however, the former, while requiring significant acreage, are remote from one another. Airlines and marine transportation are similar in that there is sizeable investment at origins and destinations; there is no private ownership of their rights-of-way, specifically air corridors and the open sea (Garrison and Levinson 2014).

In contrast, railroads are required to own their own rights-of-way (although there are exceptions where ownership is a government unit, especially with regard to passenger railroads) and incur major initial investment as well as ongoing maintenance costs. While each mode has its own particular infrastructure requirements, each of those components needs to be protected from both natural and man-made harm.

Protection from What?

Infrastructure needs to be protected from both natural and man-made incidents; however, these

Critical Infrastructure: Transportation Systems, Table 1 Taxonomy of threats

	Natural events	Man-made events
Rapid onset	Lightning strikes	Accidents
	Earthquakes	Terrorist attacks
	Floods	
	Tornados	
	Flash floods	
Moderately rapid onset	Hurricanes	
	Blizzards	
	Ice storms	

Source: Adapted from Young and Peterson (2014)

may occur across a wide scale of magnitude. A taxonomy of such incidents is found in Table 1 where the speed of incident onset is also an important consideration.

The variables of speed of onset, location, scale, timing, and whether the incident is natural or man-made have a clear bearing on how and to what extent a particular element of infrastructure needs to be protected. Note, too, that protection needs to be considered both when the particular asset is built and during its useful life.

Several factors are related to the need to protect transportation infrastructure and while this list is not intended to be exhaustive, they nevertheless need to be considered (Young and Peterson 2014):

1. Speed of onset is to also suggest a modicum of unpredictability with regard to timing, magnitude, location, and frequency (or regularity of threat).
2. The extent to which multiple infrastructure components are affected at any particular time. An example would be the loss of a specific bridge plus a nearby power station, both used by an electrified commuter railroad.
3. High stakes – in other words, human life is threatened, or are people's physical well-being adversely affected
4. The infrastructure component is either so large or complex that its damage or destruction will require a lengthy period of time to repair or replace
5. The infrastructure component is in a remote location where equipment, personnel, and needed materials are not easily accessed?
6. There may be cascading impacts such as when a tsunami is triggered by an earthquake or that a terrorist organization may take advantage of a natural disaster occurrence.

Public Policy and the National Infrastructure Protection Plan

Through much of US history, the protection of infrastructure has been highly fragmented with the key exceptions being during wartime when key elements warranted specific extra protection as was the case with those port areas that were embarking troops or war materiel. A specific case during World War II was the Pennsylvania Railroad's Horseshoe Curve in Western Pennsylvania, which at the time handled a disproportionately high volume of freight destined to the European front. Its importance was such that Germany actually landed a team of saboteurs tasked with the curve's destruction – fortunately the plan never came to fruition, the agents were captured, tried, and executed (Plant and Young 2007).

In the post-9/11 era, concern over all manner of terrorist activity prompted the formation of the National Infrastructure Protection Plan (NIPP 2013). With the realization that there is so much infrastructure deemed critical, both public and private sector owners and operators have been encouraged to make risk-informed decisions in order to arrive at the most effective solutions for allocating the necessary resources to protect the infrastructure. To take a direct quote from the NIPP:

> While individual entities are responsible for managing risk to their organization, public-private partnerships improve understanding of the threats, vulnerabilities, and consequences of how to manage them through the sharing of indicators and practices and the coordination of policies, response, and recovery activities. (NIPP 2013)

With the number of public and private entities involved, it is reasonable to recognize that different entities will have different tolerances

for risk depending on their specific business plans, resources, and regulatory environments. Protecting infrastructure, therefore, becomes a matter of applying risk management practices of both government and industry within the constraints of available resources and incentives and the range of consequences (Lee 2009).

The NIPP needs to be considered as the cornerstone for transportation infrastructure protection. To paraphrase its key tenets:

1. Risk needs to be identified and managed in a coordinated way in order that security and resilience resources can be efficiently allocated. Security and resilience need to be considered joint being the security can be thought of as preventing an occurrence and protecting the infrastructure element as well as limiting the impact in the event of an occurrence.
2. The understanding and addressing of risks from cross-sector dependencies and interdependencies is essential. It is essential that different sectors understand one another. For example, the nation's railroads operate as individual corporations, but they also function as a network. This means that during the normal course of business, they interchange freight cars in order that a shipment can move from one coast to the other by transiting the rails of multiple firms. In similar fashion during, for example, a natural disaster or a man-made act such as sabotage, entire trains or individual freight cars can be routed on competitors' lines in order that the disruption to the supply chain is minimized.
3. Cross-community information sharing is essential. Cross-community is defined as public and private sectors but also across industries. Transportation is a derived demand activity that means that there is an inherent relationship between transportation service providers and their respective shippers and consignees.
4. The importance of particular units of critical infrastructure transcends national boundaries thus requiring cross-border collaboration, mutual assistance, and other forms of cooperative agreements.
5. Many if not most supply chains are now global, meaning that the interdependency between US interests and those of foreign partners is inseparable. Firms are increasingly aware that their success may not just be dependent upon their tier-1 suppliers but that tier-2, tier-3, and tier-n may pose a considerable previously unrecognized risk. Consequently, with that many tiers of concern, the vulnerability can be significant as transportation infrastructure embracing multiple modes are employed. Between transporting raw materials, semifinished components for further assembly, and finished goods, today's products may wind up traveling thousands of miles before ever reaching the consumer (Supply Chain Council 2017).
6. Security and resilience need to be considered when assets, systems, and networks are being designed. Consideration must be given to determining the most effective and efficient approaches to identify, deter, detect, disrupt, and prepare for threats and hazards, mitigate vulnerabilities, and minimize their consequences. Building resilience into the infrastructure can be thought to be a, if not the, major consideration (McDougall and Radvanovsky 2008).

The NIPP received a major boost when the issue of critical infrastructure was emphasized in the Presidential Policy Directive 21 (PPD 21) in 2013. PPD 21 unscored the importance of critical infrastructure as a key element in national security but also for the nation's economic well-being as well. Moreover, it charged 11 key federal agencies with developing critical infrastructure security and resilience functional relationships for 16 industry sectors, evaluating the public-private partnership model, identifying systems requirements to enable information sharing, developing a situational awareness capability, and the creation of a national research and development plan. While the term critical infrastructure encompasses a broad spectrum of assets, the key agencies of interest in this encyclopedia entry are the Department of Homeland Security and the Department of Transportation, specifically the Transportation Security Administration (TSA) (PPD-21 2013).

Cataloging Critical Infrastructure and Key Resources

Before being able to address intermodal infrastructure, the magnitude of the nation's transportation infrastructure needs to be assessed on a mode-by-mode basis including the types and quantities of assets required by each, identification of the owners, whether such assets are capacity constrained, and the interrelationships existing between them. The details for beginning such discussion are found in Table 2.

Of particular interest to transportation infrastructure is the often expensive elements that include bridges, tunnels, and the information and control systems necessary for controlling the flows of traffic across the network. The details for these are found in Table 3.

The investment in transportation infrastructure is immense; hence. Even the task of arriving at some quantitative measures is a daunting one. Nevertheless, such is necessary in attempting to understand the nature of US infrastructure and to determine the enormity of the undertaking in protecting it. Table 4, using an assortment of information sources, both public and private, seeks to establish such detail.

Transportation as Networks: Multimodalism and Interdependence

In the above table, there are several notes concerning modes of sharing rights-of-way, terminals, and other infrastructures. While this does pose problems with regard to statistics, it also means that multiple entities will need to address the risk assessments as well as determine the priorities that must be addressed with respect to security and resiliency. Up to this point, the issue of intermodalism and multimodalism have not been addressed; however, these themes are increasingly cogent given, for example, that many truckers now rely on the railroads for their long-distance hauls and the ocean marine carriers are highly dependent on them for the inland movement of containers, both for export and import (Garrison and Levinson 2014; Price and Hashemi 2016).

Understanding the NIPP Framework

The foregoing discussion assessed in broad terms the transportation infrastructure both qualitatively and quantitatively. Because transportation infrastructure has such long useful lives, most protective measures will be retrofitting, often when major maintenance is being undertaken. Moreover, lesser maintained and deteriorated infrastructure makes for more attractive targets for terrorists and more subject to damage from natural disasters than well-maintained infrastructure. The following, shown below as Fig. 1, is a visual portrayal of the NIPP framework and is useful for guiding discussion.

Note that this framework was developed for broad application across all sectors of the economy and can be used in all geographic regions and by a wide range of partners. As with the discussion on transportation infrastructure, there may be government or private sector owners and/or operators involved, and both are always stakeholders. This means that using the model to establish priorities requires a public-private partnership whereby risk is not only assessed, but investment is considered along with the potential use of alternative assets and resources. The NIPP makes a critical point when it states that:

> Risk management enables the critical infrastructure community to focus on those threats and hazards that are likely to cause harm, and employ approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration. (NIPP 2013)

Step 1 of FEMA's critical infrastructure risk management framework speaks to the establishment of goals and objectives that are established at the sector level; however, the most difficult and perplexing aspect of transportation in general and its infrastructure in particular is that it touches every aspect of the economy and in all manner of the health and well-being of the population. There is no sector that is unaffected by transportation inasmuch as it affects food, communications, clothing, shelter, education, energy, finance,

Critical Infrastructure: Transportation Systems, Table 2 US transportation links and nodes infrastructure and its ownership

Mode	Right-of-way	Ownership	Terminal facilities	Ownership	Notes
Aviation	Air corridors	Federal government	Hub airports	State and local government; quasi-governmental authorities	
			Secondary commercial airports		
			General aviation airports	As above plus private ownership	
Inland waterway	Dredged rivers	Federal government	Barge terminals	Private ownership	[a]
	Canals	Federal and state government	Ferry terminals	State and local government; quasi-governmental authorities; private ownership	
Ocean maritime	Dredged rivers and harbors	Federal government; state and local government	Container terminals	Ports authority and private ownership	[b]
			Bulk terminals		
			Cruise and ferry terminals		
Pipeline	Petroleum	Private ownership	Terminals and pumping stations	Private ownership	
	Natural gas				
	Chemicals				
	Water	State and local government, quasi-governmental authorities; private enterprise		State and local government, quasi-government authorities; private enterprise	[c]
Railroad – freight	Main lines	Private ownership although some government ownership exists	Railyards, intermodal terminals	Private ownership	[d]
	Secondary lines				
	Branch lines				
Railroad – Passenger	Main lines	Federal, state, local and quasi-governmental authorities	Stations, railyards	Federal, state, local, and quasi- governmental authorities	
	Secondary lines				
	Branch lines				
Roads and highways	Interstate limited access	State and local government; quasi-governmental authority, some private sector (toll roads)			[e]
	Main arterials				
	Secondary				

Notes:
[a]The majority of barge traffic is for bulk materials; hence, loading/unloading is at shipper or consignee facilities
[b]Port size may vary considerably depending on channel depth and terminal capacity
[c]Excluded are service distribution lines to individual homes and industry
[d]Some branch lines may be owned by local or regional governments with operations leased to others
[e]Municipal streets intended for local traffic are excluded

Critical Infrastructure: Transportation Systems, Table 3 US transportation: major elements and information infrastructure (excludes rights-of-way)

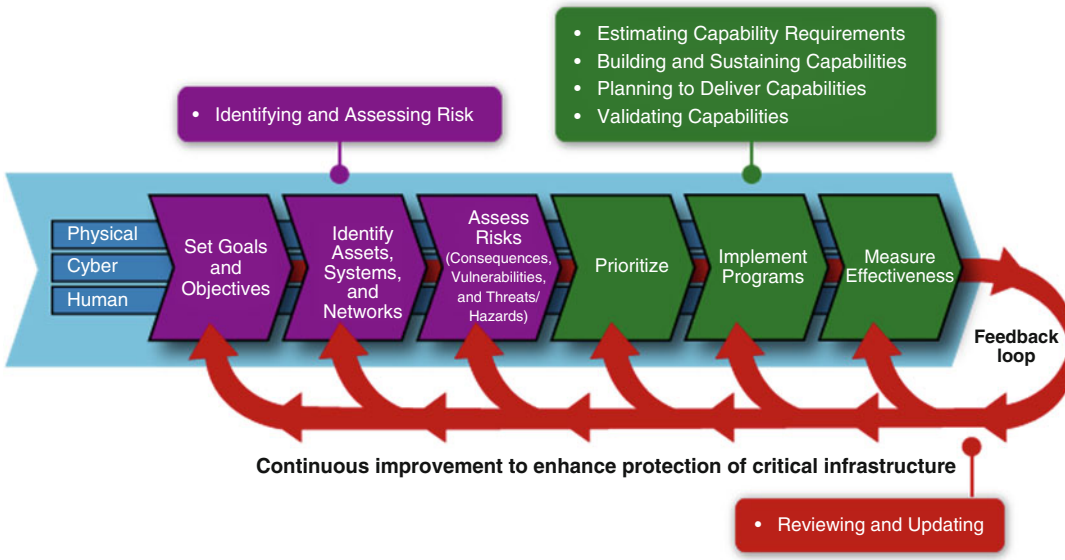
Mode	Major infrastructure	Ownership	Information infrastructure	Ownership	Notes
Aviation	Runways	State and local government, quasi-governmental authorities, private ownership	Air traffic control system	Federal government	[a]
Inland Waterway	Locks	Federal government, quasi-governmental authorities	Aids to navigation (e.g., buoys), lock traffic control systems	Federal and state government, quasi-governmental authorities, private enterprise	[b]
Ocean maritime			Aids to navigation (e.g., buoys and lighthouses)	Federal government, private industry	[c]
			Traffic control systems		
Pipeline	Booster stations	State and local government, quasi-governmental authority, private ownership	Traffic control systems	Private ownership	
Railroad – freight	Large-span bridges	Same as under right-of-way in Table 2	Communication and signaling systems	Private ownership	[d]
	Secondary bridges and culverts		Freight car location systems	Private ownership	
	Tunnels				
Railroad – Passenger	Large-span bridges	Federal, state, local, and quasi-governmental authorities	Communication and signaling systems	State, local, and quasi-government authorities	
	Secondary bridges and culverts				
	Tunnels				
	Electrified line catenary or third rail				
Roads and Highways	Large-span bridges	State and local government; quasi-governmental authority	Traffic control systems	State and local government, quasi-governmental authorities	
	Secondary bridges and culverts				
	Tunnels				

Notes:
[a]Ground traffic control systems are maintained locally
[b]Waterways may be marked by government-owned aids to navigation (ATONs) or in industry-maintained waterway, as with many bulk terminal facilities, by private aids to navigation (PATONs)
[c]Government-operated traffic control systems are used in busy ports and crowded waterways
[d]North American railroads employ radio-frequency identification systems for locomotives and cars. Information exchange between railroads is governed by a joint venture for which the railroads are owners

Critical Infrastructure: Transportation Systems, Table 4 Key US infrastructure components by mode

Mode	Type	Number	Notes
Aviation	Hub airports plus those for commercially served communities	5,388	Usually operate some general aviation
	General aviation airports	19,500	
Inland waterway	Canal miles	25,500	
Ocean maritime	Ports	179	
	Bulk terminals	Not differentiated	
Pipelines	Petroleum, petrochemical, and natural gas	2,400,000	
Railroads – freight	Track miles	223,000	Does not include miles, freight railroads operate over passenger railroad-owned tracks
	Bridges	100,000	Size not differentiated
Railroads – passenger	Track miles	21,356	Passenger railroads most often tenants on freight rails
	Bridges	1,414	Size not differentiated
Roadways	Interstate and national highway miles	160,000	
	Total miles	2,678,000	Includes only paved road surface miles
	Bridges	604,000	Size not differentiated

Sources: US Bureau of Transportation Statistics, American Association of Port Authorities, Association of American Railroads



Critical Infrastructure: Transportation Systems, Fig. 1 Critical infrastructure risk management framework. (Source: Emergency Management Institute, FEMA)

utilities, and services. Services can be interpreted as private sector of government services that would include defense, police and fire protection, and even entertainment. The purpose here is not to set goals and objectives but to raise an awareness of the difficulty such a task can be with a sector that is so pervasive (NIPP 2013).

Step 2 was essentially undertaken on a macro basis in Tables 2 and 3. Key is that the description reads "identify assets, systems, and networks" given that individual assets need to function as components within systems and networks. Note that the term *systems* is meant to denote a group of assets working together as a whole and that networks are groups of systems functioning together. In a transportation example, a container yard within a port area is a particular asset, whereas adding the containership, the berths, and the gantry cranes together is the container shipping system when linked with other ports. To view such within the structure of a network, one must add the highway and rail systems that access a given port area. The partners will each have a different view of the meaning of criticality based on the respective risks involved which mean those that are required for maintaining continued operations for the delivery of goods and services to their customers (NIPP 2013).

Step 3 requires an understanding of three terms that bespeaks the need for protection:

1. Threats – natural or man-made occurrences that have the potential to harm life, information, operations, the environment, property, and the overall economy.
2. Vulnerability – some feature the leaves an asset open to exploitation or susceptible to a specific hazard.
3. Consequence – the effect that an event or incident may have including any potential cascading effect.

Combined, these provide the basis for assessing and analyzing risk. While it is advocated that each of the many stakeholders engage in this process, the reality is that it is a complex and messy affair given the large number of participants each with a different set of priorities as well as risk tolerance and financial objectives. Moreover, the complexity increases exponentially as the scope of a potential incident or event increases (NIPP 2013). For example, the loss of a single highway overpass on a rural highway in Central Pennsylvania will be very different than the loss of an interstate highway span crossing the Mississippi River. Even with such a simple comparison, the importance of that Pennsylvania incident would be different should that road be the major access to an army installation such as Fort Indiantown Gap.

Step 4 requires the actionable plans be implemented. There are no silver bullets available because identifying, detecting, disrupting, and preparing for threats and hazards can be expensive because they require personnel, physical assets, and, in many cases, the application of technology needed to both enhance security and increase resilience (NIPP 2013, Lee 2009). Examples of these in a transportation venue would include:

1. Using security protective measures to detect or delay an attack or intrusion. Several Class I railroads have begun using drones to surveil those miles of right-of-way that transit sparsely populated and remote areas. With regard to natural disasters, airlines for many years have staffed their own weather services in cooperation with the National Oceanographic and Atmospheric Administration. Moreover, Walmart, the retailer but also the operator of a very large private truck fleet, has similar resources.
2. Detecting malicious activities that threaten critical infrastructure and related operations and systems across sectors. BNSF Railway and others have engaged private citizens in their Citizens for Rail Security effort, which functions as an enlarged neighborhood watch (Young, Gordon, and Plant, p. 178). Moreover, the US Coast Guard participates in America's Waterway Watch where recreational boaters are encouraged to "see something, say something" whenever they detect activities that seem out of place (USCG Aux 2018).
3. Implementing intrusion detection and vetting measures for sensitive and mission-critical activities to prevent unauthorized access.

Implementation of the Transportation Workers Identification Card (TWIC) endeavors to credential respective personnel. In more critical activities, such as data centers and most truck terminals, specific identification measures are now commonplace and go beyond simple picture identification initiatives and may include biometric and fingerprint identification (Edwards and Goodrich 2013).

4. Monitoring facilities and networks potentially targeted for attack. Aside from the traditional closed-circuit TV monitoring that has been around for decades, more sensitive locations are installing geofencing technology that uses RFID tags to determine what or who is accessing a given area as well as those that are moving off their intended routing (Young et al. 2017).
5. Monitoring cyber systems for potential incursions into control systems such as air traffic control, train control systems, and pipeline traffic management. Defense-sensitive firms have for some time employed software that cannot only determine that attacks are occurring but in general terms who the source may be (Lee 2009).

Reduction of vulnerability is a practice that works equally well for both natural and man-made threats. Consider the following:

1. Build security and resilience into the design and operation of assets, systems, and networks. For a recent example, tank cars used for hauling crude oil underwent significant specification improvement that includes double-walled vessels and protection of related appurtenances because protecting infrastructure can also be a matter of improving the vehicles operating over transportation infrastructure (Edwards and Goodrich 2013).
2. Improving siting of infrastructure to avoid those areas prone to natural disasters or susceptible to exploitation. While this sounds obvious, its implementation may prove difficult especially with regard to maritime operations where access to deep water, both for channels and port facilities, is a prerequisite for attracting the services of, for example, container lines.
3. Develop and conduct training exercises to raise awareness and understanding of common vulnerabilities and potential mitigation approaches. Airport transit and passenger railroads have long engaged in such practices, and a common approach to mitigation is mutual aid agreements between first responders (Lee 2009).
4. Develop contingency plans for those events that have a higher likelihood of occurring. Railroads have long had agreements to use the tracks of competitors in the event of a disaster. This was seen numerous times when Gulf Coast hurricanes damaged stretches of track or bridges. Another example is the hurricane and tsunami evacuation routes posted in many coastal areas (McDougall and Radvanovsky 2008).

Notice that security and safety are, while related, different concerns. Moreover, resilience need to be considered together because as with the former, the focus is on prevention and protection, whereas with the latter, it is preparedness to mitigate, respond, and recover (Zoli and Steinberg 2016).

Step 5 demands that every event be assessed with regard to the effectiveness of those measures that were employed to prevent, protect, mitigate, respond, and recover from any event where transportation infrastructure was threatened, damaged, or destroyed. An after action report needs to assess what worked and what did not. This subsequently becomes the principal component of the feedback loop that serves to inform Step 1, the modification of goals and objectives, but also each of the other predecessor steps (NIPP 2013).

Conclusion

It must be emphasized that the orderly process for protecting transportation infrastructure must be an ongoing one because the environment is a dynamic one given the following considerations:

1. Infrastructure is always in the process of being replaced, upgraded, or generally maintained but also expanded to reflect increases in demand.

2. The demands placed on a particular element of the transportation infrastructure will change over time due to changes in economics including location of competing modes of transportation, location of those demanding transportation services, and the price of fuel and economics that may be related to such variables such as the price of fuel, taxation, and demographics.
3. Demand may shift due to the actions of government including taxation, weight and size regulations governing vehicles, and land use constraints.
4. The use may be affected by changes in the way costs are assessed, which could include the establishment of tolls, raising or existing tolls, or imposing time of day congestion pricing schemes.

Cross-References

- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
- ▶ Maritime Security: Acceptable Risks
- ▶ Maritime Security: Problems of Security Versus Safety Practices
- ▶ Natural Hazards
- ▶ Rail (Train) Security
- ▶ Risk Analysis: National and International Standards

References

Edwards, F., & Goodrich, D. (2013). *Introduction to transportation security*. Boca Raton: CRC Press.

Garrison, W., & Levinson, D. (2014). *The transportation experience* (2nd ed.). New York: Oxford University Press.

Lee, E. (2009). *Homeland security and private sector business*. Boca Raton: CRC Press.

McDougall, A., & Radvanovsky, R. (2008). *Transportation systems security*. Boca Raton: CRC Press.

National Infrastructure Protection Plan. (2013). *Partnering for critical infrastructure protection and resilience*. Washington, DC: Department of Homeland Security.

Plant, J., & Young, R. (2007). *Securing and protecting America's Rail System: U.S. Railroads and opportunities for terrorist threats*. Boston: Citizens for Rail Safety.

Presidential Policy Directive-21: Critical infrastructure protection and resilience (2013). Washington, DC: The White House.

Price, W., & Hashemi, A. (2016). Seaport operations and security. In S. Hakim, G. Albert, & Y. Shiftan (Eds.), *Securing transportation systems*. Hoboken: Wiley.

Supply Chain Council. (2017). *Supply chain operations reference model (version12) quick reference guide*. Available at https://www.apics.org/docs/default-source/scc-non-research/apicsscc_scor_quick_reference_guide.pdf. Accessed 15 Aug 2018.

Talarico, L., Sorensen, K., Reniers, G., & Springael, J. (2016). Pipeline Security. In S. Hakim, G. Albert, & Y. Shiftan (Eds.), *Securing Transportation Systems*. Hoboken: Wiley.

USCG Auxiliary. (2018). America's Waterway Watch. http://www.cgaux.org/aww/php. Accessed 22 Aug 2018.

Young, R., Gordon, G., & Plant, J. (2017). *Railway security: Protecting against manmade and natural disasters*. New York: Routledge.

Young, R., & Peterson, M. (2014). Emergency management must become emergency supply chain management. *Journal of Emergency Management, 12*(2), 171–187.

Zoli, C., & Steinberg, L. (2016). Adaptive, resilience and critical infrastructure security: Emergent challenges for transportation and cyberphysical infrastructure. In S. Hakim, G. Albert, & Y. Shiftan (Eds.), *Securing transportation systems*. Hoboken: Wiley.

Further Reading

Edwards, F. and Goodrich, D. (2013). *Introduction to Transportation Security*. Boca Raton: CRC Press

National Infrastructure Protection Plan. (2013). *Partnering for critical infrastructure protection and resilience*. Washington, DC: Department of Homeland Security.

Presidential Policy Directive-21: Critical infrastructure protection and resilience (2013). Washington, DC: The White House.

Hakim, S., Albert, G., and Shiftan, Y. (eds). *Securing Transportation Systems*. Hoboken, NJ: John Wiley

Critical Infrastructure: Water and Wastewater Systems Sector

Kevin R. Gamache
Texas A&M University, College Station, TX, USA

Keywords

Critical infrastructure · Drinking water · Wastewater · Interdependencies · Homeland security

Definition

Critical infrastructure is comprised of those systems and assets, whether physical or virtual, that are so essential to a nation that any interruption could have a severe impact on national security, public health or safety, economic well-being, or any combination thereof (GAO 2011). Water and wastewater critical infrastructure includes the infrastructure necessary to transport, treat, store, distribute, and remove drinking water and wastewater and also to control water quantity and quality (Alcaraz and Zeadally 2015).

Introduction

A nation's critical infrastructure, especially its water and wastewater treatment systems, provides the foundation for supporting public health, economic vitality, and healthy environment; defines its standard of living; and is the basis for a competitive advantage compared with other nations (Alcaraz and Zeadally 2015; EPA 2017; Jacobsen 2018). The reliability, performance, continuous operation, safety, maintenance, and protection of water and wastewater systems for producing clean and safe water must be a priority (Alcaraz and Zeadally 2015) as it is essential for sustaining life (Faily et al. 2015). The average person is only able to survive 3 days without water to maintain body systems health and functionality (Birkett 2017).

Highly sophisticated and intricate technology is required to run and operate our drinking water and wastewater systems (Birkett 2017). The US Water Critical Infrastructure Sector has historically provided clean and safe water to protect public health and the environment (EPA 2017). Guided by the requirements of the Safe Drinking Water Act (SDWA) and Clean Water Act (CWA), water utility service providers have been conducting routine daily, weekly, and monthly water quality monitoring for more than 30 years; as a result, the United States has one of the safest water supplies in the world (EPA 2017).

According to the US Environmental Protection Agency (EPA), approximately 153,000 public drinking water utilities and more than 16,000 wastewater utilities across the United States provide clean drinking water to almost 84 percent of the US population and wastewater treatment to more than 75 percent of the population (EPA 2017). Across the country, these systems comprise approximately 77,000 dams and reservoirs; thousands of miles of pipes, aqueducts, water distribution, and sewer lines; and 168,000 public drinking water facilities (many serving as few as 25 customers) (Clark et al. 2011a). There are 52,000 separate community drinking water systems in the United States (Finkel 2017).

Throughout history, even as early as 3000 BC, water critical infrastructure systems have been a consistent target. Increasing global populations in the twentieth and twenty-first centuries placed significant demands on water sources and water infrastructure resulting in water critical infrastructure becoming an increasingly attractive target for terrorist attack (Birkett 2017). There is growing awareness that urban water systems are vulnerable to both human-made and natural threats and disasters such as droughts, earthquakes, and terrorist attacks (Clark et al. 2011a). Earthquakes and terrorist attacks have many characteristics in common, because both are almost impossible to predict and can cause significant devastation and confusion (Clark et al. 2011a). This entry provides an overview of the water and wastewater critical infrastructure characteristics, followed by an explanation of the interdependencies of water systems and culminating in a discussion of the risks to water and wastewater critical infrastructure systems.

Water and Wastewater Critical Infrastructure Characteristics

Water supplies are typically from groundwater, surface water, or a combination of the two. Community water systems serving fewer than 10,000 people typically utilize groundwater, whereas large community water systems obtain the majority of their water from surface sources (EPA 2017). Conveyance systems bring water from remote sources to treatment plants using pipes or

canals. These conveyance systems can utilize pumping or gravity to move water from source to destination (EPA 2017). Raw water is commonly stored in remote reservoirs or lakes prior treatment (EPA 2017). Distribution systems, which include networks of pipes, tanks, pumps, and valves convey clean water to customers. Volume and pressure are controlled within the distribution system to ensure water is delivered when and where needed (EPA 2017).

Water treatment occurs via a variety of physical and chemical treatment processes dependent upon the contaminants detected in the raw water (EPA 2017). Initial treatment processes include coagulation, flocculation, and sedimentation followed by filtration. Surface water supplies are generally treated at conventional facilities using filtration to remove particulates and pathogenic microorganisms (Clark and Deininger 2000). The filtration process is followed by disinfection using chlorine dioxide, potassium permanganate, and nano-filtration (Clark and Deininger 2000). The disinfection process eliminates disease-causing organisms such as cysts or enteric viruses (Tech Brief 2006). Finished water is stored in a treated water storage area before distribution to customers. In a few cases, treated water is stored in large, uncovered reservoirs that may be susceptible to attack or contamination (EPA 2017).

Monitoring is conducted for common regulated and unregulated contaminants. Many community water systems install sensors at critical points to monitor physical properties, such as water pressure and water quality (EPA 2017). Integrated control systems which include supervisory control and data acquisition (SCADA) systems are essential to drinking water utility operation. These electronic networks are often dependent upon wireless communication which links treatment and distribution monitoring and control systems to a central display in the operation/control room (EPA 2017). Process systems and operational controls for operations of the utility and treatment processes are provided by electronic control systems not controlled by the utility's SCADA system (EPA 2017). Non-operational control systems or enterprise systems such as customer billing, email, and other personnel-related applications and tools are also essential to the operation of water and wastewater critical infrastructure (EPA 2017).

Collection systems, which are typically networks of pipes, conduits, tunnels, lift stations, and associated equipment, convey and pump wastewater from the source to the treatment plant. Community water services usually have three types of sewers: sanitary sewers, storm sewers, and combined sewers. Treatment plant operations can vary significantly depending on the type of collection system used (EPA 2017). Preliminary treatment can include removal of foreign materials that could damage a plant's infrastructure or impair treatment operations. Usual methods of removal include the use of chemical addition, pre-aeration, bar racks, screens, shredding equipment, or grit chambers. Pretreatment processes include coagulation, flocculation, and flotation to remove particles and solids (EPA 2017). Primary treatment removes suspended and floating material. Secondary treatment reduces dissolved and colloidal organic substances and suspended matter and is commonly accomplished through the use of settling tanks to separate liquid from solids.

Flotation and other methods are also frequently used. Grease, heavy metals, solids, and nutrient are removed through chemical processing. A combination of physical, chemical, and biological processes removes or reduces nutrient and soluble organic content (EPA 2017). Disinfection processes neutralize pathogens, bacteria, viruses, and protozoan cysts in the water disinfection processes. The most common disinfection processes are chemical disinfection (most often using chlorine), ozonation, and ultraviolet (EPA 2017). Effluent can be discharged to a body of water or wetlands and to groundwater aquifers via percolation or deep-well injection, applied on land, or re-repurposed (EPA 2017). The costliest part of wastewater treatment is the handling of residuals and biosolids. Solids treatment includes thickening, stabilization, digestion, chemical, composting, dewatering, incineration, and heat drying equipment (EPA 2017).

Monitoring systems are often installed at critical points to provide visibility on a range of

physical properties like flow rates and water quality indicators and to detect levels of contaminants throughout the treatment cycle (Clark et al. 2011a). One of the most common monitoring systems is the supervisory control and data acquisition (SCADA), which is a system of software and hardware elements including wireless communications and electronic networks that link monitoring and control systems for the collection, treatment, and discharge to a central display and operations room (EPA 2017). Process systems and operational controls which include electronic control systems related to the operations of the utility and treatment processes not controlled by the utility's SCADA systems (EPA 2017) are also used. Finally, nonoperational *enterprise control systems* including customer billing, email, and other personnel-related applications and tools (EPA 2017) also play an important role in the overall process.

Critical Infrastructure Sector Interdependencies

The material flows that constitute and sustain cities (water, electricity, gas, oil, food, information, and a multitude of other commodities) have traditionally been viewed and managed separately but are increasingly becoming interconnected and co-dependent (Williams et al. 2018). In sum, water critical infrastructure has become interlinked as communities have grown and developed. Today this critical infrastructure appears as intermingled distribution webs which meet the cyclic and intermittent growth of cities, towns, and communities (Birkett 2017).

The cascading effects of denial of water sector services would result in loss of other critical services, such as firefighting and health care, as well as adverse effects in other dependent and interdependent sectors, such as energy, transportation, and food and agriculture (EPA 2017). For illustration, the water and wastewater critical infrastructure systems sector is heavily dependent upon the chemical critical infrastructure sector to perform disinfection and water treatment. The chemicals are conveyed and delivered, by the transportation sector to water CI destinations, utilizing rail, road, and marine transport (Birkett 2017). The failure to understand how disruptions to one infrastructure sector could cascade to others, exacerbate response and recovery efforts, or result in common cause failures can leave planners, operators, and emergency response personnel unprepared to deal effectively with the impacts of such disruptions (Williams et al. 2018).

Most critical infrastructure sectors are, to a certain extent, dependent on the water and wastewater treatment sector. Porod et al. (2014) identify that most other critical infrastructure sectors are dependent upon water CI and would see degradations in service ranging from 67% to 99% after 4 h of water loss (Birkett 2017). Birkett determined 75% of all US critical infrastructure could be directly impacted should the continuous supply of treated water be lost. Community water supplies deliver water under pressure and are designed to supply most of the water for firefighting purposes. Loss of water or a substantial loss of pressure could disrupt firefighting, interrupt drinking water service, and undermine public confidence (Clark and Deininger 2000). The notion that our nation's critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communication technologies (so-called cyber-based systems), is more than an abstract, theoretical concept (Rinaldi et al. 2001).

The water and wastewater sector is a lifeline sector with interdependencies to the 15 other critical infrastructure sectors. Because of the mutual dependence and interconnectedness made possible by modern information, communications, and cyberinfrastructure, our critical infrastructures are "system of systems" and are increasingly vulnerable in ways they have never been before (Gillette et al. 2002). Often spread over large geographic areas, these "systems of systems" can prove difficult to protect (Birkett 2017). Determining localized threat levels from deliberate adverse acts of human intervention or terrorism is also exceptionally difficult given the interconnectedness of the various critical infrastructure sectors (Birkett 2017).

The interdependent nature of critical urban infrastructure makes it more vulnerable to external impacts, leading to a domino effect among different assets and sectors impacting on people and places (Steele et al. 2017). Figure 1 illustrates the dependencies each of the other 15 critical infrastructure sectors have on the water and wastewater systems sector.

The manner in which the water and wastewater systems sector interacts with each of the other 15 critical infrastructure sectors is illustrated in Fig. 2.

Risks to Water and Wastewater Systems Sector

Due to the significant interdependency of the water sector with other critical infrastructure sectors, the vulnerability of a community's water critical infrastructure depends on the location and relationship of all the critical nodes comprising urban infrastructure systems, such as energy, food, water, sewage, and communications (Steele et al. 2017). Gleick (1993) commented that as civilization and development move forward in the twenty-first century, military action and instruments of war will increasingly involve water and wastewater, and water critical infrastructure will be an increasingly likely target of military or aggressive actions (Birkett 2017).

Historical examples of attacks and attempted attacks on water critical infrastructure are myriad. Terrorism is a significant threat to water security, and recent attention has turned to the potential that these attacks have for disrupting urban water supplies (Clark et al. 2011a). Terrorism in the United States was not considered a serious threat until the second half of the 1990s (Clark and Deininger 2000), but in recent times, Jihadist terrorist groups like Al Qaeda and others have shown an increased level of interest in attacks on water critical infrastructure (Birkett 2017). Recent attacks both at home and abroad have forced government planners to consider the possibility that critical elements of the US infrastructure might be vulnerable to terrorism (Clark and Deininger 2000). There were 162 documented attacks on water CI from 1980 to 2012, with a measured increase from 1970 (Birkett 2017).

Emergency response planning is inherent to the water sector because utilities have always had to respond to natural disasters. For decades, owner/operators of water sector assets have developed and improved plans to respond to human-made and natural disasters (EPA 2017). However, it was the threat of terrorism that prompted water, wastewater, and dam utilities to focus heavily on safety and security, for the protection of public health (Morley 2007). In particular, the 1995 terrorist acts in Oklahoma City and the September 11, 2001, attacks signified the need for changes in physical security of the water sector (Finkel 2017).

Aside from terrorism, security for water utilities is also concerned about two threats on the physical side: employee malfeasance from someone gone rogue and an outsider with a gun (Finkel 2017). The potential for chemical or biological contamination of water supply systems exists along with the possibility that such systems might be sabotaged (Clark and Deininger 2000). An employee with access could pollute the water, open a dam or valve when it should not be open, or power up turbines nefariously. There is a myriad of scenarios that could lead to a catastrophic event for that system (Finkel 2017). Figure 3 displays three levels of moderate, high, and significant risks to the water and wastewater treatment sector.

Numerous factors make water supply systems particularly vulnerable: they are spatially diverse; susceptible to intrusion; and component-rich (Clark and Deininger 2000). Water supply systems are generally governmental, with each supply system being highly localized (Clark and Deininger 2000). If wastewater infrastructure were to be damaged, the lack of redundancy in the sector might cause a denial of service. Disruption of a wastewater treatment utility or service can cause loss of life, economic impacts, and severe public health and environmental impacts. Regulations, research, and outreach, while extensive, have been aimed mostly at impacts on the environment and public health. Because drinking water is consumed directly, health effects

Sector	Sector Dependency on Drinking Water	Drinking Water Dependency on Sector	Sector Dependency on Wastewater	Wastewater Dependency on Sector
Chemical	• Manufacturing operations • Office operations	• Chlorine and other treatment chemicals • Office operations	• Manufacturing operations • Office operations	• Disinfectants and other critical treatment chemicals
Commercial Facilities	• Facility operations	• Bottling	• Facility operations	• Biosolids operations and distribution • Business operations
Communications	• Equipment cooling • Common rights-of-way	• Emergency communications with responders • General operations • SCADA • Monitoring	• Infrastructure access • General operations • Common rights-of way • Equipment cooling	• Common rights-of-way • Communications with emergency responders • General operations • SCADA • Remote monitoring • Communications with the public
Critical Manufacturing	• Water as a product constituent • Equipment cooling	• Operational and process equipment	• Manufacturing operations • Office operations	• Critical manufactured utility operations • Piping and infrastructure
Dams		• Storage; reservoirs • Flood mitigation	• Aquifer recharge	• Storage reservoirs • Flood mitigation
Defense Industrial Base	• Office operations • Equipment cooling	• Production of parts	• Office operations	• Production of parts
Emergency Services	• Continuity of operations • Firefighting and hazardous material spill and event responses • Decontamination services • Emergency water supplies • Equipment maintenance	• Special weapons and tactics and tactical operations • Coordination with the Incident Command System (ICS) • Law enforcement • Bomb explosive ordnance disposal • Emergency (medical and firefighting) responders • Hazardous materials (HAZMAT) responders	• Continuity of operations • Decontamination services • Infrastructure access	• Special weapons and tactics and tactical operations • Coordination with ICS • Law enforcement • Bomb explosive ordnance disposal • Emergency (medical and firefighting) responders • HAZMAT responders
Energy	• Cooling and scrubbing • Steam generation • Mining operations • Ore processing	• Process power • Pump, wells, treatment, operations • Office operations	• Waste management • Common rights-of-way • Methane generation • Cooling and scrubbing • Steam generation • Methane generation • Mining operations • Ore processing • Raw material (e.g., hydrogen production) • Refining	• Pumps and treatment; operations and repair • Office operations • Common rights-of-way • Repair and recovery operations • Process power • Delivery of components and material • Backup power requirements
Financial Services	• Office operations	• Facility financial operations, bonds, grants, loans, etc.	• Office operations	• Rates and spending authority • Research • Company operations

Critical Infrastructure: Water and Wastewater Systems Sector, Fig. 1 (continued)

Sector	Sector Dependency on Drinking Water	Drinking Water Dependency on Sector	Sector Dependency on Wastewater	Wastewater Dependency on Sector
Food and Agriculture	• Biosolids (soil amendment/fertilizer) • Irrigation • Restaurant operation • Processing plants • Water reuse	• Biosolids land application • Biomass for energy production	• Biosolids (soil amendment/fertilizer) • Irrigation • Restaurant operation • Processing plants • Water reuse	• Biosolids land application • Biomass for energy production
Government Facilities and Commercial Facilities	• Provision of public facilities • Office operations	• Rates and spending authority • Research • Company operations	• Provision of public facilities • Office operations	• Rates and spending authority • Research • Company operations
Healthcare and Public Health	• Hospital and clinic operations • Nursing home operations • Pharmaceutical, device, and supply manufacturing • Laboratory services • Transportation of equipment and supplies	• Vaccination and inoculation • Laboratory services • Information on treatment and response • Conditions for public notice • PPE donning and doffing guidance	• Hospital and clinic operations • Nursing home operations • Pharmaceutical, device, and supply manufacturing • Laboratory services • Transportation of equipment and supplies	• Hospital and clinic operations • Nursing home operations • Pharmaceutical, device, and supply manufacturing • Laboratory services • Transportation of equipment and supplies
Information Technology	• Common rights-of-way • Equipment cooling	• Common rights-of-way • E-communications with emergency responders, WARNs, etc. • Monitoring • SCADA • General operations	• Common rights-of-way • Equipment cooling	• Common rights-of-way • E-communications with emergency responders, WARNs, etc. • Monitoring • SCADA • General operations
Nuclear Reactors, Materials, and Waste	• Cooling and scrubbing • Office operations • Reclaimed water	• Power delivery	• Common rights-of-way • E-communications with emergency responders, etc. • Monitoring • SCADA • General operations	• Power delivery
Transportation Systems	• Office operations • Common rights-of-way	• Delivery of treatment chemicals • Operations, maintenance, and repair • Delivery of components and materials • Company operations • Transport of emergency responders and equipment • Common rights-of-way	• Office operations • Common rights-of-way	• Delivery of treatment chemicals • Operations, maintenance, and repair • Delivery of components and materials • Company operations • Transport of emergency responders and equipment • Common rights-of-way

Critical Infrastructure: Water and Wastewater Systems Sector, Fig. 1 Critical infrastructure sector interdependencies. (Adapted from 2015 water and wastewater sector-specific plan, US EPA 2017, Appendix 4, pages 40–42)

associated with contamination have long been major concerns. Besides, interruption or cessation of the drinking water supply can disrupt society, affecting human health and such critical activities as fire protection that can have significant consequences to the national or regional economies. The public correctly perceives drinking water as central to the life of an individual and of society. Consumers are highly sensitive to the threat of contamination or disruption (EPA 2017).

Although wastewater may not be an obvious critical security concern, there are clear environmental implications if poorly treated water would be pumped into waterways (Faily et al. 2015). There are more than 16,500 publicly owned treatment works (POTW) in the United States that

Sector	Water & Wastewater Systems Interaction
Chemical	EPA coordinates risks associated with the storage, transport, and use of chemicals in water utility operations. Water and Wastewater Sector owners and operators coordinate with federal, state, and local authorities to ensure compliance with chemical safety regulations.
Commercial Facilities	Water and wastewater utilities provide services necessary to the operations of commercial facilities.
Communications	Water and wastewater utilities must ensure communication between first responders during emergency management operations.
Critical Manufacturing	Water and wastewater utilities provide services necessary to the operations of manufacturing facilities, including a source of water for cooling or other processes.
Dams	Dams and reservoirs provide water for a significant fraction of the population. EPA coordinates with dam owners and operators including DOI that have responsibility for managing the Nation's dams and reservoirs, including pumping plants, canals, and pipelines.
Defense Industrial Base	Water and wastewater utilities provide services necessary to the operations of defense facilities.
Emergency Services	At the operational level, water utilities ensure that emergency responders have sufficient information to respond effectively to incidents at their facilities.
Energy	EPA also coordinates with the Federal Energy Regulatory Commission (FERC), which regulates interstate transmission of natural gas, oil, and electricity. EPA's interactions with FERC primarily involve the Water and Wastewater Sector's interdependency with electric power.
Financial Services	Water and wastewater utilities often utilize bonds, loans, and grants to fund operational changes and infrastructure upgrades.

Critical Infrastructure: Water and Wastewater Systems Sector, Fig. 2 (continued)

Sector	Water & Wastewater Systems Interaction
Food and Agriculture	With the issuance of HSPD-9, USDA expanded its role with the EPA to build upon and increase current monitoring and surveillance programs that provide early detection and awareness of the disease, pest, and poisonous agents.
Government Facilities and Commercial Facilities	Water and wastewater utilities provide services necessary to the operations of government facilities.
Healthcare and Public Health	With the issuance of HSPD-9, USDA expanded its role with the EPA to build upon and increase current monitoring and surveillance programs that provide early detection and awareness of the disease, pest, and poisonous agents. Water and wastewater utilities coordinate with public health agencies during emergency response and other water quality-related events, as well as provide services necessary for the operations of medical and other healthcare facilities.
Information Technology	DHS National Cybersecurity Division (NCSD) oversees the protection of the IT industry and also has a cross-sector responsibility regarding the security of industrial control systems that are critical for all sector operations.
Nuclear Reactors, Materials, and Waste	Water and wastewater utilities provide services necessary to the operations of nuclear facilities, including a source of cooling water.
Transportation Systems	The Water and Wastewater Sector shares several key interdependencies with DOT, including its reliance on the Transportation Systems Sector to provide chemicals, such as gaseous chlorine, and supplies for drinking water and wastewater treatment facilities. Highways and railways can also present vulnerabilities to the Water and Wastewater Sector where they pass near or over sources of drinking water.

Critical Infrastructure: Water and Wastewater Systems Sector, Fig. 2 Water and wastewater systems interaction with other CI sectors. (Source: Adapted from *2015 water and wastewater site-specific plan* (EPA 2017), Appendix 4, pages 42–44)

collectively provide wastewater service and treatment to more than 227 million people and are generally designed to treat domestic sewage (EPA 2017). Non-domestic industrial users also discharge effluent into collection systems for subsequent treatment at a POTW and are subject to the national pretreatment program (EPA 2017). According to Bahadur and Samuels (2011), damage to the nation's wastewater facilities or collection systems could result in loss of life; catastrophic environmental damage to rivers, lakes, and wetlands; and contamination of drinking water supplies (Clark et al. 2011a). Disruption of a wastewater treatment services can cause loss of life, economic impacts, and severe public health and environmental incidents. The lack of redundancy in the wastewater sector might cause a denial of service if wastewater infrastructure were to be damaged. The public is much less sensitive to the possible exploitation of wastewater infrastructure vulnerabilities compared to drinking water vulnerabilities (EPA 2017).

Most Significant Risks
• Natural disasters (such as impacts on water and quantity from floods, hurricanes, earthquakes, ice storms, pandemic flu, and other geographic catastrophes) • Economic implications of aging infrastructure • Cyber events • Capability in managing an area-wide loss of water Note: Although the Water Sector has been defined as a lifeline Sector, this is not commonly recognized among all relevant stakeholders, a situation that can escalate consequences during area-wide events.
High Risks
• Economic costs of preparing and response: The Water Sector can create a substantial economic risk in a disaster, but there are insufficient funds to prepare for and address risks ahead of time • Ignorance about the consequences of inaction and apathy from some stakeholders in utilities, the customer base, state/local government, and Federal Government/Congress • Inadequate coordination and information sharing during preparation, response, and recovery • Intentionally malicious acts • Limited resource availability: Many utilities for competing for needs (e.g., regulatory, aging infrastructure, environmental and public health protection, and workforce succession requirements) that are immediate, concrete and can limit resource availability for implementing preparedness and resiliency improvements • Unenforced and outdated requirements that do not address evolving threats.
Medium Risks
• Lack of mutual aid agreements, effective education, and outreach to emergency management, and lack of best practices for emergency response planning • Technology interoperability issues that create information-sharing challenges during the response • Insufficient communication to water utility boards of the definition, management, and prioritization of the critical assets and needs

Critical Infrastructure: Water and Wastewater Systems Sector, Fig. 3 Risks to the water and wastewater treatment sector. (Source: Adapted from the 2013 roadmap to a secure and resilient water and wastewater sector and 2015 water and wastewater sector-specific plan)

Conclusion

In the United States, society relies on the water and wastewater treatment systems to live, and this sector shares a significant interdependency with the other critical infrastructure sectors (EPA 2017; Jacobsen 2018). The vulnerability of a community's water critical infrastructure depends on the location and relationship of all the critical nodes comprising urban infrastructure systems, such as energy, food, water, sewage, and communications, and interruption would result in a cascading adverse effect (EPA 2017; Steele et al. 2017). There is growing awareness that urban water systems are vulnerable to both human-made and natural threats and disasters such as droughts, earthquakes, and terrorist attacks (Clark et al. 2011a). Moreover, increasing global populations in the twentieth and twenty-first centuries placed significant demands on water sources and water infrastructure, resulting in water critical infrastructure becoming an increasingly attractive target for terrorist attack (Birkett 2017).

Cross-References

- ▶ Critical Infrastructure Protection
- ▶ Hazardous Environmental Effects
- ▶ Homeland Security Act of 2002
- ▶ Industrial Control System
- ▶ Insider Threat
- ▶ SCADA

References

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53–66.

Bahadur, R., & Samuels, W. B. (2011). Wastewater critical infrastructure security and protection. In R. M. Clark, S. Hakim, & A. Otsfeld (Eds.), *Handbook of water and wastewater systems protection* (pp. 87–102). Dordrecht: Springer.

Birkett, D. M. (2017). Water Critical Infrastructure Security and Its Dependencies. Contemporary Voices: St Andrews Journal of International Relations, 8(2), pp. 1–21. https://doi.org/10.15664/jtr.1289

Clark, R. M., & Deininger, R. A. (2000). Protecting the nation's critical infrastructure: The vulnerability of U. S. water supply systems. *Journal of Contingencies and Crisis Management, 8*(2), 73–80.

Clark, R. M., Hakim, S., & Ostfeld, A. (2011a). *Handbook of water and wastewater systems protection*. Dordrecht: Springer.

EPA, U. S. (2017). *2015 water and wastewater sector-specific plan*. Retrieved December 16, 2018, from https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

Faily, Shamal & Stergiopoulos, George & Katos, Vasilios & Gritzalis, Dimitris. (2015). "Water, Water, Every Where": Nuances for a Water Industry Critical Infrastructure Specification Exemplar. https://doi.org/10.1007/978-3-319-33331-1_20

Finkel, E. (2017). Essential to life, critical to keep secure: Water, wastewater and dam authorities toil under public radar to guard precious resources. *Spotlight on Critical Infrastructure*, 54(2), 42–43.

GAO, U. S. (2011). *Critical infrastructure protection cybersecurity guidance is available, but more can be done to promote its use: Report to congressional committees*. Washington, DC: Government Accountability Office.

Gillette, J. L., et al. (2002). Analyzing water/wastewater infrastructure interdependencies. No. ANL/DIS/CP-107254. Argonne National Lab.

Gleick, P. H. (1993). *Water in crisis*. New York: Oxford University Press.

Jacobsen, L. B. (2018). Keeping watch over our vital water infrastructure. *Journal-American Water Works Association, 110*(8), 54–56.

Luiijf, Eric A. M., & Marieke H. A. Klaver. (2004). Protecting a nation's critical infrastructure: the first steps. IEEE International Conference on Systems, Man and Cybernetics, (2), 1185–1190.

Morley, K. M. (2007). A vision and direction for water sector security and preparedness initiatives. *Journal-American Water Works Association, 99*(2), 38–42.

Porod, C., Collins, M., & Petit, F. (2014). Water Treatment Dependencies. *CIP Report, 12*(14).

Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K., & J. I. E. E. E. C. S. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25.

Steele, W., Hussey, K., & Dovers, S. (2017). What's critical about critical infrastructure. *Urban Policy and Research, 35*(1), 74–86.

Tech Brief. (2006). Disinfection, National Drinking Water Clearing House, West Virginia. http://www.nesc.wvu.edu/pdf/dw/publications/ontap/2009_tb/disinfection_DWFSOM50.pdf

Williams, J., Bouzarovski, S., & Swyngedouw, E. (2018). The urban resource nexus: On the politics of relationality, water–energy infrastructure and the fallacy of integration. *Environment and Planning C: Politics and Space*, 0263774X18803370.

Further Reading

Clark, R., Hakim, S., & Ostfeld, A. (2011b). *Handbook of water and wastewater systems protection*. New York: Springer.

Hamada, M., & Koike, T. (2015). *Critical urban infrastructure handbook*. Boca Raton, FL: CRC Press.

Lewis, T. (2015). *Critical infrastructure protection in homeland security* (1st ed.). Hoboken, NJ: Wiley.

Critical Infrastructure Protection

Ronald L. Martin
Capital Technology University, Laurel, MD, USA

Keywords

Critical Infrastructure Protection, CIP · National Infrastructure Protection Plan, NIPP · Presidential Policy Directive, PPD · Presidential Decision Directive, PDD · DHS · InfraGard · CSS · CIIP · NIST · NCCoE · resilience · PCCIP · SLTT · HSPD · CISA · QHSR · Patriot Act · NIHS

Definition

In the United States

The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely, systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Presidential Policy Directive-21 (PPD-21, 2013)

PPD-21 defined critical infrastructure. The final piece of this subject is protection. Protection is "Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters." (PPD-8, 2011)

Introduction

As defined above Critical Infrastructure Protection (CIP) of key infrastructures is essential to maintaining our way of life. The CIP programs must be of the highest priority of a government and its citizenry. The US government organizes the nation's critical infrastructure into 16 categories or sectors. Where the United States defines 16 sectors, the international community defines a global approach to a framework. The Center for Security Studies (CSS) published in 2009 the International Critical Infrastructure and Information Protection (CIIP) Handbook (CIIP 2009). This entry will focus on the US CIP Program. However, since the United States is a part of and is within the CIIP Handbook, the international framework will be discussed.

The international and the US approaches used the same baseline study initiated by the United States. The premise for both programs used the findings of the US President Commission on Critical Infrastructure Protection (PCCIP) of 1997. The PCCIP summarized two attack modes toward critical infrastructures. These modes are attacks against physical and cyber of essential targets to infrastructure (PCCIP 1997).

The US DHS is the focal point for CIP initiatives. However, the National Institute for Standards and Technology (NIST) is contributing to the nation cybersecurity governance. NIST established the National Cybersecurity Center of Excellence (NCCoE). As with the national CIP Program, NCCoE is a public-private partnership. This partnership provides cybersecurity solutions for an aspect of the US CIP Program.

The International CIIP Framework

The CIIP framework and program is the result of a research effort conducted by the Center for Security Studies (CSS) at ETH Zurich. The 2008/2009 International Handbook published the findings of this research. The CSS handbook investigated the critical infrastructure programs of 25 countries. Additionally, they analyzed the essential policies of infrastructures of the seven international organizations. This research used the US President's commission on critical infrastructure protection of 1997 (PCCIP 1997) as its basis. The PCCIP Report commissioned by President William Clinton appointed Robert T, Marsh as the commission's chairman. The commission report identified risks and vulnerabilities to infrastructures.

Additionally, the PCCIP report summarized the mode of attack to critical infrastructure targets in two domains. These attack domains are physical and information (Cyber). Therefore, the CSS found that information is a part of critical infrastructure protection and not a separate assertion. Thus, the term critical infrastructure and information protection (CIIP) is essential. As the CSS researched the 25 countries and reviewed the initiatives of 7 organizations, they emphasized the CIIP construct (CIIP 2009). The PCCIP Report identified targets as facilities, people, media, financial, computers, and information.

The research involved a review of 25 countries using 5 focus areas. The first area was to define how the surveyed country defined critical infrastructure. They then reviewed each country's policies and initiatives; CSS reviewed the country's organizational structure and evaluated

the country's public outreach and involvement; and finally, they assessed country's governance (CIIP 2009). By using these focus areas within their research approach, CSS normalized the comparative analysis of the surveyed country and the international approach to the protection of critical infrastructure.

The final step of the CSS research reviewed open-source material and collaborated with national experts from academia and government-related experts. This step utilized the knowledge, skills, and outreach of 7 internationally known organizations.

The US CIP Program Evolution

Like the international effort shown by the CIIP framework, the US program became formalized after the issuance of the PCCIP Report of 1997. In May 1998, President Clinton issued Presidential Decision Directive number-63 (PDD-63). PDD-63 established a national goal for the United States. This goal provided a framework for a public-private partnership to mitigate infrastructure vulnerabilities. To that end, the directive designated federal executive agencies to lead sector governance base on the agency's mission (PDD-63). The most significant action from the instruction was the establishment and the appointment of the national coordinator for security, infrastructure protection, and counter-Terrorism (PDD-63 1998, p. 11). In the ensuing years, the nation was working with the national coordinator to mitigate vulnerabilities to infrastructures. Following the events of the terrorist acts of September 11, 2001, the nation increased its efforts toward physical protections (CRS 2012 and 2015). As these protection efforts progressed, the US Congress became increasingly interested in the efforts that the nation was undertaking. The US Congress directed the Congressional Research Service (CRS) to research the activities surrounding critical infrastructure protection. John Moteff, a CRS specialist in science and technology policy, reviewed two historical products. CRS published the first in 2012. Its title is critical infrastructure resilience: The Evolution of Policy and Programs and Issues for Congress (CRS R42683 2012). Contained within this report was the definition and measurement of resilience. The report refers to resilience as ". . .the ability of a system to resist, absorb, recover from, or successfully adapt to a change in environment or conditions. . ." (CRS R42682 2012 summary page 1).

The 2012 report summarized the actions made under the Presidents Bush and Obama administrations. Upon the election of President Bush, his administration continued the initiatives started by the Clinton administration (CRS RL30153 2015). The National Security Council was reorganized into 17 policy coordinating committees (PCC) (CRS RL30153 2015). Eventually, the management and oversight for counter-terrorism and national preparedness, PCC was established within the executive office of the president (EOP). The next action the administration took was the establishment of the federal chief information officer (CIO) under the EOP deputy director of the office of management and budget. This position would serve in an oversight role of the federal agency's CIOs. During the same period, the Department of Defense chartered a commission on national security/21st century (USCNS/21) in 1998. This commission was also known as the Hart-Rudman Commission (or Taskforce). The Hart-Rudman Commission released its findings on January 31, 2001. The significance of these findings was that after the terrorist attack of September 11, 2001, President Bush established the Department of Homeland Security, as recommended by the report (CRS RL30153 2015).

The President Bush Administration issued high-level policy documents. They were the National Strategy for the Physical Protection of Critical Infrastructure and Key Resources (2002), Homeland Security Presidential Directive 7 (2003), and the National Infrastructure Protection Plan (NIPP) (2006). However, these documents did not adequately address resilience (CRS 2012).

Under the President Obama administration, resilience was integrated with the homeland security policy. In February 2010, the Quadrennial Homeland Security Review (QHSR) referenced

resiliency. The QHSR identified five core missions. These missions are:

> Mission 1: Preventing Terrorism and Enhancing Security
> Mission 2: Securing and Managing Our Borders
> Mission 3: Enforcing and Administering Our Immigration Laws
> Mission 4: Safeguarding and Securing Cyberspace
> Mission 5: Ensuring Resilience to Disasters (QHSR 2010, pp. 14–15; DHS Annual Report 2010)

With the addition of resiliency to the program, the subsequent NIPP publications strengthen not only preparedness but resiliency. Also, under the President Obama administration, DHS issued two revisions of the NIPP (2009 and 2013). Each revision prompted the development of CIP Sector plans. It was these efforts by the two formers presidents that formed the current US Critical Infrastructure Protection program.

The US Critical Infrastructure Protection Program

The US and the international CIIP programs formally started after the publication of the PCCIP Report of 1998. In the previous section of this entry, President Clinton issued PDD-63. PDD-63 outlined the infrastructures that require protection. These infrastructures are critical in that disruption; it would cause adverse consequences to the welfare of the United States (PDD-63 1998). In the wake of the terrorist attack on September 11, 2001, President Bush passed into law on October 26, 2001, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. The acronym USA Patriot Act is a shortened description of this act. In late 2006, the US Government General Accountability Office (GAO) found that most of the nation's critical infrastructure is owned and operated by a state, local, tribal, territorial (SLTT), and private organizations (GAO 07-39 2006). As such, this places a unique governance responsibility on the US federal government to provide informative governance to the critical infrastructure community. Contained within the 2006 NIPP, the following notation stated: "Private sector owners and operators are encouraged to participate in the NIPP partnership model and to initiate protective measures to augment existing plans for risk management, business continuity, and incident management and emergency response in line with the NIPP framework" (NIPP 2006, p. 9). Note, unless otherwise codified by statute, conformance with US federal governance is only encouraged.

In as much as the preponderance of critical infrastructure resides outside of the US federal government, the Federal Bureau of Investigation (FBI) established a program named InfraGard.

> InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within the critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's membership includes business executives, entrepreneurs, lawyers, security personnel, military, and government officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security. (InfraGard 2018)

The InfraGard program establishes seamless interaction between the private sector, SLTT government entities, and the federal government. This interaction facilitates information sharing with the critical infrastructure 16 sectors. The FBI Office of the Private Sector oversees the InfraGard program.

To review the evolution of the US National Infrastructure Protection Plan (NIPP) Sector program, a review of the issued NIPP documents will show the history. The first NIPP issued in 2006 identified 17 sectors aligned with Homeland Security Presidential Directive 7 (HSPD-7) (NIPP 2006). The next NIPP released in 2009 identified 18 sectors aligned with HSPD-7 (NIPP 2009).

In 2013 Executive Order (EO) 13636 of 2013, titled Improving Critical Infrastructure Cybersecurity, issued and directed (in-part) the executive branch of government to strengthen cybersecurity

practices and share cyber threat information (EO 13636). The US Presidential Policy Directive 21 (PPD-21) established the 16 critical infrastructure sectors and aligned them with a federal government agency. These agencies referred to as sector-specific agencies (SSA). The current NIPP issued in 2013 identifies 16 sectors aligned with PPD-21. The 16 sectors are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems (NIPP 2013).

According to the Cybersecurity and Infrastructure Security Agency (CISA) of the DHS website, the challenge program leverages the innovative research programs from DHS Science and Technology initiatives. Over the years 2016, 2017, and 2018, the challenge program has resulted in innovative recommendations from the public sector to advance CIP from a technological perspective (source: https://www.dhs.gov/cisa/nipp-security-and-resilience-challenge#wcm-survey-target-id).

CISA partnered with the National Institute for Hometown Security (NIHS). The below quote will show the purpose of this relationship.

> NIHS provides an opportunity for the critical infrastructure community to help develop technology, tools, processes, and methods that address immediate needs and strengthen the long-term security and resilience of critical infrastructure. https://www.thenihs.org/

Through this relationship and the challenge program, CISA provides the critical infrastructure community innovative research and solutions.

The National Cybersecurity Center of Excellence

As the nation becomes increasingly reliant on our cyber infrastructures, the National Institute of Standards and Technology (NIST) established the National Cybersecurity Center of Excellence (NCCoE). According to the NCCoE website, the goals of NCCoE are "...to provide practical cybersecurity, to Increase the rate of adoption, and to accelerate effective innovation..." (source: https://www.nccoe.nist.gov/about-the-center/strategy).

According to the NCCoE website, currently, eight projects relate to CIP sectors. These projects are consumer/retail, energy, financial services, healthcare, hospitality, public safety/first responder, transportation, and manufacturing. NCCoE refers to these projects as "use cases" (source: https://www.nccoe.nist.gov/projects/use-cases).

With the NIST involvement through the NCCoE will provide to the critical infrastructure community a directed approach to cybersecurity.

Conclusion

Since the early beginnings of characterizing certain infrastructures as critical, countries of the world are working toward making our planet a safer place to exist. Through the CIP and CIIP programs are providing the framework for this protection. The citizens of the industrialized world depend on multiple infrastructures to assure sustainment of their welfare. The total population has had and will continue to have an essential role in providing security to the facilities of these infrastructures. In the United States, the government has provided and continues to provide a framework for the nation to view and interact with infrastructures that are critical to the survivability of the country. The nexus shown between the US DHS, NIST, and CSS provide a different view of the CIP environment. This entry has provided a synthesis of the founding of CIP, internationally, as well as the approaches to analyze and implement infrastructure protection.

Cross-References

- ▶ Critical Infrastructure: Commercial Facilities Sector
- ▶ Critical Infrastructure: Critical Manufacturing Sector

- ▶ Critical Infrastructure: Defense Industrial Base Sector
- ▶ Critical Infrastructure: Emergency Services Sector
- ▶ Critical Infrastructure: Government Facilities Sector (GFS)
- ▶ Critical Infrastructure: Nuclear Reactors, Materials, and Waste Sector
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector

References

Bush. (2003). Homeland Security Presidential Directive 7 (HSPD-7) 7: Critical infrastructure identification, prioritization, and protection. The Executive Office of the president. Washington, DC. https://www.dhs.gov/homeland-security-presidential-directive-7

Center for Security Studies, ETH Zurich. (2008–2009). International CIIP handbook. http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf

Commission on Critical Infrastructure Protection. (1997). Critical foundations protecting America's infrastructure, The report of the President's commission on critical infrastructure protection. https://fas.org/sgp/library/pccip.pdf

Critical Infrastructures Protection Act of 2001, 42 U.S. Code § 5195c. Critical infrastructures protection, Section was enacted as the Critical Infrastructures Protection Act of 2001 and also as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 or USA PATRIOT Act. https://www.law.cornell.edu/uscode/text/42/5195c

Cybersecurity and infrastructure security agency (2018). Critical Infrastructure Sectors. U.S. Department of Homeland Security. Washington, DC. https://www.dhs.gov/cisa/critical-infrastructure-sectors

Department of Homeland Security. (2003). Homeland security Presidential directive 7: Critical infrastructure identification, prioritization, and protection. Washington, DC. https://www.dhs.gov/homeland-security-presidential-directive-7

Department of Homeland Security. (2006). National Infrastructure Protection Plan (NIPP). Washington, DC. https://fas.org/irp/agency/dhs/nipp.pdf

Department of Homeland Security. (2009). National Infrastructure Protection Plan (NIPP) Partnering to enhance protection and resiliency. Washington, DC. https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Department of Homeland Security. (2013). National Infrastructure Protection Plan: Partnering for critical infrastructure protection and resilience. Washington, DC. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Department of Homeland Security. (2018). Cybersecurity and infrastructure security agency, Critical Infrastructure Sectors. Washington, DC. https://www.dhs.gov/cisa/critical-infrastructure-sectors

Department of Homeland Security – Fiscal year 2010 Annual financial report. (n.d.). Washington, DC. https://www.dhs.gov/xlibrary/assets/cfo-afrfy2010-vol1.pdf

Gharehyakheh, A., Tolk, J., Fritts, S., & Cantu, J. (2017). A survey paper of protecting critical infrastructure: Applying high reliability theory to advance organizational resilience. IIE Annual Conference. Proceedings, 1968.

Moteff, J. (2012). Critical infrastructures: background, policy, and implementation, issues for congress (CRS R42683) Congressional Research Service, (CRS). Washington, DC. https://fas.org/sgp/crs/homesec/R42683.pdf

Moteff, J. (2015). Critical infrastructures: background, policy, and implementation, (CRS RL30153) Congressional Research Service (CRS). Washington, DC. https://fas.org/sgp/crs/homesec/RL30153.pdf

National Cybersecurity Center of Excellence. (2018). Accelerating the deployment and use of secure, standards-based technologies, brochure National Institute of Standards and Technology. Gaithersburg, MD. https://www.nccoe.nist.gov/sites/default/files/library/nccoe-brochure.pdf

National Cybersecurity Center of Excellence. (2019a March). Strategy. https://www.nccoe.nist.gov/about-the-center/strategy

National Cybersecurity Center of Excellence. (2019b March). Projects: Use cases. https://www.nccoe.nist.gov/projects/use-cases

National Infrastructure Protection Plan. (2013). Partnering for critical infrastructure protection and resilience. Washington, DC: Department of Homeland Security.

Office of the Press Secretary. (1998). Critical Infrastructure Protection presidential decision directive/NSC-63 (PDD-63). The White House. Washington, DC. https://fas.org/irp/offdocs/pdd/pdd-63.pdf

Office of the Private Sector. (2018). Office of the Private Sector (OPS) Fact sheet. Federal Bureau of Investigation. Washington, DC. https://www.fbi.gov/file-repository/ops-factsheet-8-3-18.pdf/view

Office of the Secretary. (2010). Quadrennial Homeland Security Review (QHSR). U.S. Department of Homeland Security. Washington, DC. https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf

Cultural Institutions Security

Mark DeMario and John Balestrieri
John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Cultural institutions · Art Museums · Libraries · Aquariums · Botanical Gardens and arboretums · Historical Sites · Monuments · Art Theft · Keywords Training · Guard Deployment · Physical Security · Special Events · Exhibitions · Constructions · Fire and Life Safety · Law and Legal Issues

Definition

Cultural property protection involves the complex and far-reaching issues securing a wide range of institutions. This entry primarily deals with museums; however, the concepts and considerations can be extended to the types of institutions which have numerous references, legal, and industry standards.

Introduction

Cultural property protection is a vast topic that includes an array of variables to consider. They face the same threats as every other public institution with the added complexity of protecting collection items while making them accessible to a wide range of visitors from school children to researchers. The items that need protection may be the property itself, irreplaceable art or artifacts, living animals or plants, and in some cases items in open public spaces. Events in the early part of the twenty-first century have resulted in a rise in violent attacks on artwork and at cultural properties of all types along with the overall increases in crimes including loss of human life. The value of art, insurance, and liability issues have necessitated a more serious focus on security in cultural properties. An incident of any kind can affect an institution's reputation with the public, groups, or other professional organizations. These may impact attendance; the ability to get loans, funding, or grants; increases in insurance premiums; and the ability to secure loans.

Types of institutions are:

1. Museums
2. Libraries
3. Aquariums
4. Botanical gardens and arboretums
5. Historical sites
6. Monuments

Personnel and Hiring of Security Force

The responsibility of any Security Director is to staff the security team with competent and able individuals. This task starts with the hiring process. The first step in that process is to post the position on any of the various job websites that provide suitable candidates for any position. The resumes must be read and analyzed to find the right candidates for the position. Suitable applicants are then scheduled for interviews. The number of resumes is then parred down to a manageable number; thus, interviewer starts the interview process. The interviewer must begin by stating the requirements of the position. It is important to point out the need to be available to work weekends, holidays, evenings, and nights. If the candidate is not willing or able to meet the basic requirements of the position, the interview should be terminated.

Once the basic requirements are met, the in-depth part of the interview begins. The questions poised must be able to draw out the personality of the candidate without being too intrusive. Questions should include the candidate's experience, the history of employment, gaps in the employment list, etc. In addition, the candidate must be articulate, well-mannered, and present a professional

appearance. The interviewer should review all pertinent documents such as DMV license (if required), address verification, security license, employment authorization card (EAD) or green card, military discharge papers (dd214),testimonial letters, passport, and training certificates. During this process it must be established that the applicant is legally able to work in the United States. The interviewer must ascertain if the candidate has the ability to act independently when necessary based on the policies and procedures of the institution.

Once the candidate is chosen, the Human Resource Department must perform a background check to include criminal, financial, education, and employment. The candidate must present three references which must be verified.

When background and references are confirmed and found to be acceptable, the Security Director or Manager must ensure that the candidate's licenses and permits are valid and up-to-date. Once the process is satisfactorily completed, the candidate will be notified with an offer of employment and a starting date confirmed.

Guard Staffing, Training, and Deployment

Perhaps, the most overlooked and underappreciated aspect of cultural property protection is the uniformed security officer or guard. The human element is essential to any modern well-run and efficient security program. A well-trained officer can prevent almost any damage, theft, or problem that may arise on a cultural property floor. It is entirely up to the institution as to whether the officers are armed or unarmed. If they are armed, the institution must ensure that they are licensed and nave completed any required training deemed necessary by the licensing agency.

The guards must be well dressed in uniforms that ensure the public has the ability to see them in a crowded gallery or area. The uniforms should consist of a jacket, slacks, white shirt, tie, and black shoes. A patch of insignia of the institution is usually located on the pocket of the jacket or the sleeve. The uniforms should point out the authority of the guard while not being too militaristic. If the guard has outdoor post duties, the appropriate gears such as parka with insignia, jacket, and rain gear must be issued, as well as necessary equipment including flashlights, electronic post-monitoring equipment, and hats.

Training

Once the candidate is hired, the training regimen is commenced. In most states, each security guard must be licensed. The training for the license consists of an 8-h pre-employment training and a 16-h post-employment training. Additional, annual 8-h training is required in order to maintain the guard's license. Each institute must conduct training sessions tailored to the specific site. The guard must be trained on fire safety, including location of fire exits, exits in the building, location and type of fire extinguishers, emergency and evacuation procedures, customer service training, and conflict resolution. Additional training by reputable professionals should be included to inspire, educate, and motivate security personnel. An in-depth insight at fire, emergency, and customer service training is covered later in the chapter (Nemeth 2018).

The guards should be well informed regarding the collection they are protecting. The presence of guards not only protects the collection, but they are fine representative of the cultural institution. In almost every museum, the security guard is the first and last member of the museum staff that is visible to the visitors. The modern-day museum guard must possess the necessary skills to handle diplomatically school children visitors on a class trip, the high-end donors, and everyone in between. In order to obtain these skills, the uniformed guard must be trained. This training is not universal in its approach. Each museum, library, and other cultural institution is unique unto itself, and thereby, the training must be specific to the building or site to which they are assigned. Additional information regarding training can be found later in the chapter.

Staffing

The Security Director or Manager has two options when hiring security guards. The choices are to hire propriety guards or contract ("rent") guards, both having its advantages and disadvantages.

The propriety guard is hired by the institution. There three advantages of employing guards in this manner rather than renting them through a third party. First the guards are trained by the security management staff at the institution, allowing them to become well versed and knowledgeable in the operation and use of the building in which they working in. Second they will develop a sense of loyalty to the institution and feel as though they are an integral part of the staff. Third propriety guards have the advantage of generous compensation packages including annual vacation, sick time, healthcare coverage, retirement plans, and sometimes even tuition reimbursement.

There are three disadvantages to hiring propriety guard. First the cost of employing a propriety staff is much more than a contract company. Second the administrative challenges are many, sick time, vacation time, and disciplinary matters. Third some guards are governed by union contracts that are negotiated and must be adhered to. All of these are a burden on the hiring institution.

In contrast, the advantages of contracting with a company is that it is generally less expensive to the institution as the agreed upon price is paid and all other costs (e.g., equipment, uniforms, compensations packages) are absorbed by the contract company. The contract company deals directly with the union both contract and any other problem. The advantage of a contract company is that the hiring institution does not have to abide by formal disciplinary procedures to deal with unsatisfactory performance. The contract guard benefit package is generally less costly to the hiring institution. Another disadvantage is that contract guards have no loyalty or commitment to the institution that they are assigned. This can create a lackluster performance. They are generally less trained and, for the most part, not well versed in security practices and procedures. If a contract firm is used, the hiring company must check that the contract companies' certificate of insurance is up to date and a copy must be maintained by the Security Director. In addition the hiring company must establish what equipment the contract company is responsible for, i.e., flashlights, uniforms, radios, etc. The contract firm must provide and keep an updated list of the guard's licenses and other pertinent information.

Many museums employ the hybrid system. They hire a staff of propriety guards and supplement them with contract guards. This has a different set of advantages and disadvantages. The favoring factors are that the number of contract guards can vary according to the needs of the institution. For example, a museum has a popular exhibition without a sufficient number of propriety guards to protect the exhibition. The museum hires contract guards to fill the void for the duration of the exhibition. When the exhibition ends, the contract guards are dismissed. This is a cost savings to the museum. The disadvantage is that contract guards are compensated less than propriety guards and are performing the same functions. This leads to conflicts between the guards and can cause personal problems among the guards, thus causing substandard protection of the collection and the visitors.

Guard Deployment

The standard policy for almost every museum is to have a guard within eyesight of each piece of art or display.

Some institutions have adopted the roaming guard policy. This policy dictates that guards roam from one gallery to another, thereby leaving art pieces unprotected and open to theft, damage, or other problems. The roaming guard concept is a result of money-saving attempts by the institution. Another money-saving attempt is to hire gallery attendants to replace security guards. These attendants are not routinely trained in fire safety, emergency methods, and first aid practices; they are generally less observant.

These cost-saving measure places the collection, visitors, and staff in jeopardy. The risk is too high to consider. It takes just one individual with nefarious intentions to not only ruin a priceless piece of art but also damage the reputation of the museum or cultural institution.

Physical Security

The Security Director or Manager is tasked with the responsibility of protecting the priceless

pieces of art, artifacts, antiquities, books, manuscripts, and sometimes living assets. This is predominantly performed by the guard staff and assisted by the use of physical exterior and interior security. Exterior security includes, but not limited to, fencing, camera (night vision) bollards, gates, and barriers. Interior security includes, but is not limited to, doors, locks, stanchions, cameras, motion detectors, access control, and glazing, to name a few. Each of the aforementioned should be utilized on a site-specific manner.

Exterior: The area directly in front of the building or site that is being protected should be clear of any obstructions. Shrubs, trees, debris, etc. should be cleared away from any door, gate, or other entrance. Parking lots should not be directly adjacent to the building or site. Parking lots should be a safe distance from the building in order to provide adequate security.

Perimeter lighting is an essential element to any physical security plan. Based on the type of institution, the lighting should be tailored to produce sufficient lighting to protect the area from intrusion and also provide a sense of security and safety to staff and visitors. There are minimum standards for lighting various spaces. *See* the Illuminating Engineering Society of North America, Guidelines for People, Property and Public Space. There are several types of lighting that are used for certain applications. They are as follows:

- Incandescent (generally used in home or offices this type is being phased out by the government)
- Mercury vapor lamps
- Metal halide
- Sodium vapor lights
- Quartz lamps
- LED
- Electroluminescent
- Halogen

Fencing

Zoos or wildlife parks are one such venue that require exterior fencing. The use of fencing, moats, and glass enclosures protect the public from animals, insects, birds, reptiles, and them from the public. When installing chain-link fencing for spaces other than zoos or wildlife refuges, the fencing should meet the US Department of Defense specifications. *See* their website for more information. When installing fencing or enclosures for zoos or wildlife refuges, see the Zoological Association of America Standards 2016. For the safety of the animals, staff, and visitors within the museum arena, the use of stanchions is more prevalent than other cultural properties. Well-placed stanchions act as barriers to protect art work. However, many museums curators frown upon their use believing they detract from the public's ability to properly view and enjoy the art. This is a continuing dilemma for the security professional and the museum's curatorial staff. Another method of protection is the use of sandpaper tape. This tape is placed on the floor in front of the art work. It can easily be stepped over, but it acts as a deterrent to keep the public at arms distance away.

Glazing

Many pieces of art are protected by glazing. Glazing is the process of placing a piece of museum glass over and existing piece of art. This glazing not only protects the art from the intentional or unintentional touching from the public, it also protects the art from harmful UV sunlight rays that may damage the art. Again, some artists refuse to allow this process adding an extra burden to the security professional.

Doors and Locks

Doors and locks are the most common and one of the best methods of protecting priceless works. The use of doors should be limited to protecting areas of the museum that are not accessible to the general public. Each of these entranceways should be equipped with electronic means of operation, i.e., card access (electronic access will be discussed later in the chapter) allows the security staff to limit access to areas and the ability to monitor said space to record who entered and what time the space was entered. If the institution uses a traditional lock system (key), the security department must maintain an up-to-date key register. Keys should never be issued unless they are approved by the department head and authorized by the Security Director.

Bollards and Barriers

Stone planters decorated with colorful flowers, shrubs, etc. line front of buildings. These planters or bollards serve a dual purpose. First they protect the area from any attempt to drive a vehicle through the front, side, or rear of the building. They are an effective method of stopping a terrorist from carrying out their attacks, plowing into the building with a bomb. Second, they add a sense of beauty to the area. There should also be intrusion-protective devices, drum-type barriers, retractable barriers, and sliding gates used at entrances to parking areas to prevent vehicles from entering secure areas (Nemeth 2018).

The Security Director along with the Facilities Manager must be aware of the potential threat of someone attempting to sabotage the building's HVAC systems. Precautions must be taken to protect all vents, access pipes, and other building access ports.

Cameras, access control, motion detectors, glass protection, as well as any other electronic security devices will be covered later in the chapter.

Alarms and Electronic Systems

Intrusion, Perimeter, and Specialty Alarms

The use of electronic alarms and surveillance has become an integral part of cultural property security and has greatly expanded the ability to monitor items or spaces with degrees of accuracy well beyond what can be accomplished by staff alone. Ideally, there would be multiple independent systems in place with overlapping coverage (in case of the event that one is compromised, intentionally or accidentally). The system should be self-monitoring and programmed to issue a warning if there is a breach or failure. It should also be supervised on-site and through an off-site central station with contact to local law enforcement, fire service, museum management, and any other preselected contacts in the event of an emergency.

Video Surveillance

Technological advancements have greatly expanded the use of video systems to monitor a space or object, serve as a deterrent, or aid in investigating an incident. Through the use of intelligent video technology, cameras can be used effectively to isolate spaces and monitor conditions, license plates, faces, persons, etc. This is especially important when critical or large areas need to be covered. Integrating alarm and access control systems with the video system can also be used to verify staff locations and record detailed activities, criminal, or otherwise.

States of Operation

A sound foundation of cultural property protection (CPP) requires a complete knowledge of the institution, personnel, structures, and grounds along with a properly trained staff as well as having the necessary policies, procedures, and systems in place. Understanding the various states of operation is essential to anticipating and preparing for the inherent risks CP face. Some circumstances may require additional or specialized staff, inspections, procedures, and the notification of outside agencies (i.e., fire service, insurance carriers, etc.).

The first four normal states of operation present well-understood risks which are handled with policies and procedures specific to the institution (Liston 1993). The last two special states present a number of risks which must be identified in advance. In all cases, emergency plans must be developed and practiced in advance since they can occur in any state.

The six states of operation are as follows.

State 1: Open to Staff and Public

This state is an institution's normal operating business hours. During this state of operation, both public visitors and everyday staff – office, shop, concessions, etc. – may be present.

State 2: Open to Staff, Closed to Public

This state covers any time staff members are expected to be at the institution, but the institution is not open to the public.

State 3: Closed to Staff, Open to Public

This state is when the institution is open to the public, but most of the staff is not present. This

state primarily covers public hours when office or back of house staffs are not present.

State 4: Closed to Staff and Public

This state is when the institution is closed to everyone. The only people in the building should be museum facilities and security staff as well as any other personnel essential to the operation of the facility and may include researchers or persons working on special projects.

There are, however, two special states that present additional risks and need to be considered.

State 5: Special Events

Basic special events such as tours, lectures, group visits, or meetings that occur during normal business hours are usually well handled with simply providing additional security to that event (if necessary). Larger and more complex events or those that extend into back of house spaces or take place after hours require coordination with internal and external parties. They sometimes expose the institution to potential problems, for example, outside personnel access to ordinarily restricted spaces, deliveries, storage of items, and removal of materials, equipment, or debris. Preparation, consumption of food, alcohol, and generally dealing with guests on site that may be there for purposes other than viewing the collection may present issues in terms of behavior or expectations. Special events also may include photo or film shoots, which may present risks inherent with having equipment or persons in close proximity to collections. Making sure all special events are separated from visitors (if possible) and do not disrupt the visitor experience be should be anticipated. Most events require coordination between departments, such as public relations, operations, exhibition design, visitor services, conservation, and, of course, security.

State 6: Construction Projects

Construction projects within the institution or with adjacent structures present a host of situations that may put the structure, collection visitors, or staff in jeopardy. Access for workers and material, in addition to the inherent risks of construction operations, require careful coordination with all internal and external stakeholders. While each project is unique, the security department is usually tasked with monitoring several key activities. Protection of the staff, guests, institution, and collections is the overall responsibility of the security department. Access control, fire system operation, life safety alarm systems, as well as threat of and response to emergencies are among the primary responsibilities of the security department. Proper planning should include modifications to standing policies and procedures which address the special additional concerns. These adjustments should address access issues, changes to normal operating procedures, and emergency response. This may require additional or specialized staff and training. They should include a site safety plan, trained construction safety personnel, and fire guards. Regular staff should also receive specialized training if they would need to access spaces as part of their regular work or in emergency situations. During the state of construction projects, the security department will work closely with construction managers, facilities, conservation, exhibition design, and any other departments involved with the project.

Protection of Collections

Exhibition

Security's place in the protection of the collection is varied in that they must protect the collection or borrowed work and still allow the visitors to view and enjoy the art. Additionally, security is responsible for the protection of the cultural institution's collection when it is not on exhibit.

There are certain fundamental precautions and procedures that must be instituted by the security department to deter or prevent anyone from causing damages intentional or unintentional to the collection on exhibit. The use of guards, stanchions, sandpaper tape, vitrines, tethering to the wall, museum wax, and glazing is some of the

traditional methods of protection an exhibition. For more information, refer to the American Museum Association. The use of cameras, motion detectors, and RFID tags (radio-frequency ID tags) is employed by many institutions to protect the collection.

Security must be knowledgeable as to the number and demographic makeup of the visitors. Is the exhibition appealing to a younger visitor – teen and/or child? If so, there are procedures that must be followed. Are strollers or baby carriages allowed on the exhibition floor? Are the children permitted to roam about unattended? For elderly or physically challenged visitors, are there wheelchairs, etc.? If a particular exhibition is popular, there should be a limit as to the number of visitors permitted in a gallery to avoid art damage and avoid emergency evacuation problems. School tours are a vital component of most museums. Guards must be assigned to every school tour that visits the museum. The uniformed guards must be well informed as to the value of each piece of art. They must give special attention to said pieces.

When an exhibition is borrowed (most museums lend and borrow art exhibits), the Security Director, in coordination with the Registrars, is committed to the borrowing policies set forth by the lending institution. Policies may call for a particular piece of art to be assigned to a dedicated guard during business hours and also during special events or tours that may take place. In addition, they may require special alarms, cameras, or RFID tags. If the piece is moved, an alarm is sounded and security is alerted. Some borrowing requirements are so stringent that they require that everyone be searched prior to entering the gallery.

Storage of the collection is another proponent of the protection of the collection. Every museum acquires art by purchase or from donations. These priceless pieces when not on exhibition must be stored. The storage facility must be temperature and humidity controlled, protected from fire, flood, theft, and any other disaster, natural or man-made. The storage site must be unobtrusive in nature, i.e., no signage indicating what the site is. The site must have state-of-the-art intrusion protection, early warning fire and smoke detection, and sprinkler systems that extinguish a fire and, at the same time, prevent any extensive water damage to the collection.

Admittance to the site must be limited only to the employees. The employees must be vetted and complete a background check. This must include a criminal, financial, and character investigation. When the facility is closed, no one should be permitted entry unless previously approved by the Head of the Curatorial Department after consulting with the Security Director.

Protection of Collections: Off-Site, In Transit, and Loans

Protecting collection pieces when not in the primary facility is complex since the control of the location and resources are harder to manage and maintain. Standard Facilities Reports used to record and verify a wide range of information about the institution, it's physical structure, security, fire, climate control, provisions for handling and packing, insurance, previous temporary exhibitions, and loans. In order to provide the same level of care there must be a full understanding of possible risks and vulnerabilities. Then planning and providing manpower and physical and electronic security, all other logistical considerations to accomplish the task must be implemented. In some cases, the collection pieces are exterior monuments or exist on extensive grounds or in parks. In other cases, the off-site location may be a storage facility, a research laboratory, or archeological site. The security plan should be developed, along with the subject matter experts, taking into consideration laws and customs, and with the cooperation of local governmental and emergency response providers. In all cases, financial planning is an essential part of the plan.

Collection sites are any location, active or inactive, where specimens, artifacts, or remains are collected. They may include archeological, underwater, previous civilization, or burial sites. Legal issues involve access permits, protests, as well as poachers, criminal activity, and vandalism. Collection sites on public roads, parks, and city streets require special plans to separate and protect both assets and the public from related activities. Specialized training, licenses or staff may be required;

each should be considered and planned well in advance. Transportation, communications, living accommodations, and medical care also need to be provided depending on site location. Emergency response and evacuation plans especially for remote or difficult locations must be completed and exercised.

In-transit protection of collection pieces, artwork antiques, documents, animals, plants, etc. is of great concern due to the additional risks presented while traveling. Factors to consider while preparing a risk analysis are value, vulnerability, distance, insurance requirements, and legal issues. The means and methods of transportation, requirements for care, environmental considerations, and packing are established by subject matter experts. The security arrangements are made along with the security management team after considering insurance, legal, and jurisdictional requirements. Care should be exercised in making travel arrangements in addition, accommodations for protection of items being transported, and overnight security, if necessary. Provisions may include armed or unarmed security escorts, climatized storage facilities, and emergency response while in transit. Maintaining communication with staff assigned to monitor movement and having continuous GPS tracking is common providing real-time tracking of personnel, vehicles, and cargo. Emergency and contingency planning should also be included.

Borrowed art, collections, objects, specimens, etc. are a primary concern for security and may require additional protection planning delineated in the loan agreement. These will be considered while preparing the lender's loan agreement and outlining, among other things, security and insurance requirements. They may also cover transportation requirements, escorts, documents, and import/export custom-related issues, which are usually coordinated through exhibition management staff along with security management. Exhibition designs that require the removal of existing collections, and the insertion of new ones, present a number of logistical and security-related issues, considering that the objects or specimens are most vulnerable to damage or theft while being handled, packed, or transported. Access and credentials for movers, couriers, and staff to restricted areas must be strictly controlled.

Construction

Security management must consider short- and long-term considerations from design considerations, through construction and commissioning, and into operation. All of these issues affect the construction costs and, as importantly, the operating costs. Local or national codes and regulations dictate the bare minimum required for occupancy, access, evacuation, fire, and life safety; however, they do not address the specific needs of cultural institutions. A comprehensive security survey must be prepared to determine project requirements. The survey should include access, guard placement, technology, and operating costs. By including security management and consultants who are experts in the cultural property protection field, changes, or even more costly retrofits, can be avoided. In addition, peer reviews are another frequently used method to ensure that the project is considering the myriad of threats and issues inherent in construction projects. The issue of construction on adjacent properties must also be carefully considered since they can affect site access and present a long list of hazards to staff, guests, collections, and the institution itself. In the case of any construction or renovation project, special security provisions should be made for day-to-day operations as well as emergency scenarios.

Security involvement in internal and external renovation or construction projects is well beyond the realm of ordinary access issues. Security management must be involved in every phase of the project.

Environmental Considerations

Environmental monitoring and control are most often handled by facilities and the exhibition staff with the advice of the conservation staff within well- documented criteria, i.e., custom details for the specific pieces. American Society of Heating, Refrigeration and Air- Conditioning Engineers

(ASHRAE) Applications 2015 includes a section on Museums, Galleries, Archives, and Libraries. The most fundamental environmental conditions are temperature and humidity. While not always critical to the collection, extremes conditions can present problems for guards and staff potentially affecting their performance, health, and well-being. Awareness of and possible exposure to gasses or chemicals used in laboratories, conservation, shops, or other day-to-day operations that security officers may encounter should also be considered. Carbon monoxide and combustible gas sensors should be incorporated in areas where these may be present. Security officers working alone, or in contained spaces, such as guard booths or patrol vehicles, should be further trained as to risks, detection, and prevention. Security staff should be trained on other environmental factors which could be hazardous to themselves, other people, and the collection, which may include animals, plants, etc.

In some cases, security personnel may be involved in completing environmental checks since they can easily be incorporated to normal rounds and inspections. Security should be trained as to how to identify and report environmental abnormalities. This should include water leaks, odors, or any other situations which differ from the norm. Training must include how to deal with exposure to harmful materials they may encounter while doing their normal work. In the event of an emergency, training should be in adherence to regulatory agencies and good industry practices and proper notifications, such as staff, emergency, and hazmat responders.

Fire, Life Safety, Emergency Planning Business Continuity

Fire

Museums are vulnerable to fire and the threat of fire then most other cultural institutions. Museums, libraries, house and exhibit books, and art works by their very nature are ignition sources for fire. Every institution must have in place a viable and up-to-date fire safety plan. The fire safety plan must be written and updated regularly. Changes in exhibitions will cause different paths of egress within gallery spaces. Roles must be defined and updated on a continuous basis. The fire plan must include every department and staff member. Fire prevention is everyone's duty and responsibility.

Fire plans must include a trained hierarchy of to respond to alarm and fire conditions and may include designated personnel such as an incident commander, wardens, searchers, and a fire brigade if appropriate. A comprehensive fire prevention plan must be developed and rigorously followed. The plan should include daily, weekly, monthly, and annual inspections to assure that the entire property is free from hazards and that all equipment and systems are fully tested and operational. Fire drills and training for all personnel is essential.

Sprinkler systems in various configurations are the most common type of fire suppression systems used in cultural institutions and include sprinklers, pre-action, and mist and in some locations deluge systems. Selection of the appropriate system must take into consideration what is being protected and the risk of collateral damage. Special extinguishing agents may be needed especially in laboratories, conservation, food preparation areas, or where high value or irreplaceable items are stored or exhibited. In some cases, low-oxygen environments or other specially designed environments should be utilized. Conversely, some locations may not require any suppression system at all but should still be considered and agreed to by all institutional partners and confirmed with local authorities and insurance company.

Fire Alarm Systems

Fire alarm systems are necessary in most CP environments and must be maintained and monitored continuously. An on-site fire alarm panel is used to monitor and collect information, annunciate alarms, communicate with off-site central station, and activate the fire suppression system. Fire alarm systems are usually mandated by local jurisdiction and often referred to standards, such as NFPA 909: Code for the Protection of Cultural Resource Properties and NFPA 914: Fire Protection of Historic Structures. The selection and placement of manual and automatic devices should be designed based on

the specific conditions and circumstances of the institution. Design, coordination, and integration should be done with the involvement of consultants who specialize in the field and are familiar with current codes, practices, technologies, regulations, and industry-specific standards.

Emergency Planning and Business Continuity

Emergency planning should be approached after careful consideration of risk analysis to the organization, collection staff, or guests. This is essential of preparing the overall protection plan and the emergency plan. It must be done in collaboration with the collection executive staff, conservation, and finance facilities and include the needs of all constituents. It is advisable to engage local emergency responders to familiarize them with special requirements, access, and equipment. Notification of staff and outside vendors via pre-established, procedures should be in place so that communication can be expedited. In addition, a prioritized list should be made for the relocation or in situ protection of property, artifacts, and records. Supplies of equipment and materials should be stored off-site, and arrangements for additional supplies should be planned. It is also advisable to have storage facilities and reciprocal arrangements with nearby cultural properties in the event of an emergency. The plan must be agreed to, adopted, implemented, and practiced on an on-going basis. Emergency procedures and the disaster recovery plans should cover all foreseeable disasters and emergencies.

Life Safety

The cultural property must be prepared for any type of emergency, whether it is man-made or a natural occurrence. The institution must have an emergency action plan (EAP). This plan should address any emergency other than fire which is covered in the aforementioned fire safety plan. Prior to writing an EAP, a vulnerability study should be conducted to ascertain the vulnerabilities that may affect the institution. When this study is completed, an EAP tailored to the needs of the institution can be created. The EAP should include provisions for evacuation of the site, sheltering in place, active shooter procedures, saving the collection and other valuables, alerting emergency responders, and the handling of the media. In addition to the EAP, there must be procedures for handling medical emergencies. The security staff should also be trained in first aid, CRP, and the use of AEDs (automated external defibrillators). Every emergency or fire plan requires testing, constant updating, involvement from all staff, drills, and after incident reviews to ensure that the safety and well-being of the institution is preserved.

Law and Legal Issues

Similar to the overall topic of cultural property protection, cultural property law must address all of the issues faced by other organizations with the added complexity of dealing with collection specific issues ranging from vandalism to animal rights. The primary legal issues that involve the security department are those that relate to guard actions concerning authority and responsibilities of security officers. Whether armed or unarmed, the local or national laws that outline guard actions, investigations, apprehension, detention, arrest, or use of force must be incorporated in the development of policies and procedures. In addition, security management must be aware of civil law that may affect the guard force and performing tasks such as assisting in medical situations, completing incident reports or occupational health issues. Labor law is another area often referenced due to the wide range of situations that security departments deal with.

Art law includes a wide range of issues dealing with the protection of the creative process, marketing, sale, and ownership of art. Disciplines including intellectual property, contract, constitutional, tort, tax, and commercial and international law must be considered. There are a number of laws and agreements that aid in deterrence, investigation, and prosecution of crimes committed against cultural properties. Others relate to theft, transport, sale, ownership of art, antiquities, remains, protected species, etc. (Lind et al. 2002).

The Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict (1954) and the subsequent UNESCO Convention (1999) on the Means of pProhibiting and pPreventing the iIllicit iImport, eExport and tTransfer of oOwnership of cCultural pProperty

and mission to "maintain, increase and diffuse knowledge by assuring the conservation and protection of the world's inheritance of works of art and monuments of history," (UNESCO 1994) addresses the protection cultural properties, contents, collections art, and artwork on an international level.

Subsequent to the incident at the Isabella Stewart Gardner museum in 1990, US laws have been established to aid in the investigation and prosecution of art theft crimes. The Theft of Major Artwork Statue signed in 1994 made it a federal crime to steal from museums and libraries. It defines institutions, theft, possession transport, and types and value of property covered. It gives authority to the FBI to investigate and prosecute art- or artifact-related crimes which previously were not within their jurisdiction. Interpol, Scotland Yard, along with agencies, such as, the Art Loss Registry, has strengthened the overall identification of investigation and prosecutions related to and return of missing or stolen art (Chaffinch 2008).

Conclusion

Protection of the world's most cherished works of art, artifacts, antiquities, monuments, books, manuscripts, and endangered wildlife is a challenging and onerous task which employees nearly every facet of the security field, from the basic security guard duties to employing the most sophisticated technology. The entire spectrum of security is used to ensure that the public has the ability to enjoy viewing these priceless works while continually protecting them from theft, or damage, whether intentional or unintentional.

Cross-References

- ▶ Personnel Security: Hiring
- ▶ Personnel Security: Training

References

American Society of Heating, Refrigeration and Air Conditioning Engineers – Applications. (2015). *Chapter 21: Galleries, archives and libraries*. Atlanta.

Chaffinch, L. (2008). *Chapter 10. The Federal Bureau of Investigation's art theft program*. Washington, DC: Journal of Library Administration.

Liston, D. (1993). *Museum security and protection. A handbook for cultural heritage institutions*. London: Routledge.

Lind, R., Jarvis, R., & Phelan, M. (2002). *Art and museum law. Cases and materials*. Durham: Carolina Academic Press.

Nemeth, C. P. (2018). *Private security, an introduction to principles and practices*. Boca Raton: CRC Press.

UNESCO Protocol to the Convention for the Protection of Cultural Property in the Event of Armed Conflict, The Hague May 14, 1954. Second Protocol-The Hague March 26, 1994.

UNESCO Second Protocol to the Hague Convention of 1954 Cultural Property in the Event of Armed Conflict. 1999.

Zoological Association of America 2016 Standards for Animal Fencing and Enclosures. For Safety of Animals, Staff, and visitors.

Further Reading

FBI Art Theft Program 1994 – Theft of major artwork 18 USC Sect 668.

FBI Art Theft Program 1994 – Theft of major artwork 18 USC Sect 3294.

FBI Art Theft Program 1994 – Theft from interstate shipment 18 USC Sect 659.

FBI Art Theft Program 1994 – Illegal trafficking in native American remains and cultural items 18 USC Sect 1170.

FBI Art Theft Program 1994 – Theft of Government Property 18 USC Sect 641 and 2114.

Fischer, R., Halibozek, E., & Walters, D. (2012). *Introduction to security* (9th ed.). Newton: Butterworth-Heinemann.

Layne, S. P. (2014). *Safeguarding cultural properties. Security for museums, libraries, parks and zoos*. Waltham: Butterworth-Heinemann.

Cybersecurity: Incident Response

Marie-Helen Maras
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Incident response · Cybersecurity · Digital forensics

Definition

Incident response refers to the containment, investigation, eradication, mitigation, and response to a cybersecurity threat.

Introduction

Incident response includes the policies, procedures, processes, practices, and communications that are designed to aid in the management of human, technical, and financial resources during and after a cybersecurity incident. Incident response is primarily concerned with containing a cyberintrusion and mitigating the harm caused by the cyberintrusion. Incident response plans are created with the understanding that it is not a matter of *if* a cybersecurity incident will happen, but *when* a cybersecurity incident will happen. An essential element in incident response, therefore, is planning for a cybersecurity incident to occur.

There is no one-size-fits-all incident response plan. The incident response plan of a private organization or government agency is determined by the organization/agency's mission, goals, assets, and available human, technical, and financial resources. There are, however, common elements within existing incident response plans across organizations and agencies. These elements are included in the National Institute of Standards and Technology's (NIST) Computer Security Incident Handling Guide (see Cichonski et al. 2012). Some of the key elements of incident response plans are explored in this chapter. In particular, it examines the three phases of incident response which describes actions taken prior, during, and after a cyber incident.

Incident Response Pre-planning

Pre-planning involves proper preparation to deal with incidents in the event that they occur, particularly, ensuring that the people, processes, and procedures that are needed for an effective cybersecurity incident response are in place. This pre-plan includes identifying priority assets and cybersecurity incidents to respond to; ensuring procedures are in place to respond to cybersecurity incidents; identifying the people, teams, and/or units responsible for responding to cybersecurity incidents; and having communication plans in place in the event of a cybersecurity incident.

Asset Prioritization

One of the key elements of preparation is the identification of what the organization/agency is protecting – particularly assets, which can be processes, people, information, financial capital, infrastructure, applications, knowledge, organization, and management. After the assets that need to be protected are identified, a determination is made as to which assets are critical to the functioning of the organization/agency and continuity of operations. These assets, deemed as priority assets, should be documented, categorized, and ranked. This priority determines the primary focus of protective measures taken during incident response and the order in which systems and operations resume after the incident. Priorities are not only assigned for response, they are also assigned for the recovery from a cybersecurity incident.

Incident Prioritization

After the assets are prioritized, the cybersecurity incidents that are of concern to the organization/agency are identified. Here, the categories and classifications of cybersecurity incidents are established. The categories of cybersecurity incidents vary by organization/agency. Some basic categories of cybersecurity incidents that have been provided by the US National Institute of Standards and Technology include malware (or malicious code); denial of service (DoS) or distributed denial of service (DDoS) attacks that prevent authorized use of systems, services, data, applications, and other resources; unauthorized access to systems, services, networks, data, applications, or other resources; inappropriate usage of networks and computers; and multiple cybersecurity incidents – whereby one incident actually encompasses two or more cybersecurity incidents (Cichonski et al. 2012).

The classifications of cybersecurity incidents vary by organization/agency. According to the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), classifications of cybersecurity incidents are created based on parameters, the most common of which are *impact* (i.e., the damage or harm caused to the organization/agency and, by way of extension, relevant others) and *urgency* (i.e., the speed with which the organization/agency needs to deal with the cybersecurity incident) (see ISO/IEC 27001). The intersection of these parameters is used to determine priorities. For example, cybersecurity incidents with a value of 1 have both high impact and urgency and, as such, are considered critical. Organizations/agencies should respond to these cybersecurity incidents first. Following these cybersecurity incidents, those valued at 2, 3, 4, etc. should be dealt with.

Accordingly, the prioritization of incidents to respond to is not based on the sequence of the detection of the events – meaning whatever was first detected or more generally the order in which events were detected. Instead, incident prioritization is based on "the current negative technical effect of the incident (e.g., unauthorized user-level access to data) but also the likely future technical effect of the incident if it is not immediately contained (e.g., root compromise)" (Young 2013, p. 16). For example, malware may infect one workstation (which is "the current negative technical effect") but, if not contained, can spread and adversely impact the functioning of the network (which is the "future technical effect").

Standard Operating Procedure

A standard operating procedure (SOP) for common cybersecurity incidents can assist in providing the necessary guidance on incident response, by including the policies and sequential acts that should be followed in the event of a cybersecurity incident. Standard operating procedures include the "processes, techniques, checklists, and forms used by the incident response team" (Cichonski et al. 2012, p. 8). These standard operating procedures should be as comprehensive as possible and detail not only the steps to be taken in the event of a cybersecurity incident but also the priorities of the organization/agency during cybersecurity incidents.

Roles and Responsibilities

The plan should include how the incident response team (IRT; aka, computer security incident response team or CSIRT) and other individuals involved in incident response will communicate the incident to relevant stakeholders. Another key element of pre-planning is determining who has the ultimate responsibility in the event of a cybersecurity incident. Specifically, individuals who will serve as a point of contact and have a primary role in incident response should be identified. These individuals will not only be responsible for managing the cybersecurity incident but will also be responsible for communicating the actions to be taken to deal with the cybersecurity incident. Depending on the type of cybersecurity incident, these individuals may also need to communicate with other relevant stakeholders both within the organization/agency and outside the organization/agency, especially if assistance is sought from external organizations/agencies. In addition to the aforementioned roles, these individuals are responsible for investigating indicators of suspicious or malicious cyber-activity, confirming that a cybersecurity incident has taken place or is currently taking place, and proposing technical solutions to manage the cybersecurity incident.

The composition and roles of the IRTs need to be delineated. Incident response teams can have different structures (for further information on CSIRT organization models, see Killcrece et al. 2003). For example, the central IRT handles all cybersecurity incidents throughout the organization/agency, while a distributed IRT includes "multiple incident response teams [in an organization/agency], each responsible for a particular logical or physical segment of the organization" (Cichonski et al. 2012, p. 13). Another structure is a coordinating team. This type of team may provide advice to other teams; for instance, it could be a department-wide team that provides assistance to teams that are located within particular government agencies (Cichonski et al. 2012). The

IRTs can be made up entirely of employees that belong to the organization/agency. These teams may also include contractors, who conduct outsourced work with respect to incident response. Also, IRTs can be made up entirely of outsourced individuals; in this instance, contractors are on-site (i.e., at the organization/agency) and hired to be on-site to perform incident response activities. Generally, the roles and responsibilities of relevant stakeholders during a cybersecurity incident should be identified and communicated to these stakeholders. The task that each of these individuals will perform during and after the cybersecurity incident should also be established and documented. The stakeholders who are tasked with responding to a cybersecurity incident should have the relevant knowledge, skills, and abilities (KSAs) to contain and mitigate the threat. Information about KSAs for IRTs can be found in the 2017 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (see Newhouse et al. 2017).

Communication

Proper communications are an essential element of incident response. Here, it is important to determine when to communicate information about cybersecurity incidents and in what circumstances, as well as to whom to communicate the incident and to what extent information about the incident will be revealed (Cyber Security Coalition 2015). It is also important to determine when communication to relevant stakeholders is not required, that is, when the cybersecurity incident does not need to be reported to these stakeholders (Cyber Security Coalition 2015). The method used to communicate the incident – meaning the communication means – must also be established. The individuals who will be contacted in the event of a cybersecurity incident within an organization/agency should be established. The contact information for all relevant individuals who need to be notified of a cybersecurity incident should be easily accessible and should be communicated to members of the organization/agency. What should also be communicated is when operations are to resume as normal (if these were impacted by the cybersecurity incident). This type of information is often communicated to executives, heads of departments, divisions, and units, as well as other supervisors (as needed and if deemed necessary). Within the organization/agency, some information about the cybersecurity incident should also be communicated to other employees especially if the cybersecurity incident impacted their ability to do their work (e.g., employees are unable to access the organization/agency's network and/or systems).

Having a plan to communicate information about the cybersecurity incident is essential. What is also essential is communicating the right information at the right time to the right individuals. This point applies to both internal stakeholder communications and external stakeholder communications. The policies and procedures for communicating a cybersecurity incident for internal stakeholders and external stakeholders, thus, also need to be established. With regard to internal stakeholders, the plan includes guidance on what type of information should be communicated with them. These plans often prescribe the following information to be communicated: information about what operations, infrastructure, data, and other assets were impacted by the cybersecurity incident; the type of response (i.e., the manner in which the cybersecurity incident is handled); and the expected outcome from the incident response, including anticipated short-term and long-term impacts of the cybersecurity incident (Cyber Security Coalition 2015). The information communicated depends on the cybersecurity incident. With regard to external stakeholders, depending on the cybersecurity incident and the terms of incident response plan, any of the following external stakeholders may be contacted: an affected external party; external IRTs belonging to other organizations/agencies; law enforcement agencies; the media; and Internet service provider and telecommunications providers (to name a few) (Cichonski et al. 2012; Cyber Security Coalition 2015).

The circumstances, if any, under which internal and external stakeholders are contacted and when they are contacted vary and depend on the organization/agency and the organization/agency's needs. Overall, whenever possible, those

impacted directly or indirectly by the cybersecurity incident should be contacted. Especially when communicating to external stakeholders, it is imperative that the legal, media, and or public affairs units/departments/offices within an organization/agency are involved in any external communications and that the information that is communicated is coordinated with this unit/department/office (Cyber Security Coalition 2015; Cichonski et al. 2012). The units/departments/offices that assist with communications to external stakeholders vary by organization/agency.

Communication has three basic functions: incident resolution and handling; limiting reputational harm/damage; and compliance driven (Cyber Security Coalition 2015). When the function of communication is the resolution and handling of a cybersecurity incident, the aim of communication is to transfer relevant information to other individuals who have a role and responsibility in incident response handling to contain and resolve the problems associated with the incident. When the function of communication is to limit the reputational harm or damage that could be caused as a result of the cybersecurity incident, this form of communication is directed at national and international partners, the media, the public at large, and other relevant internal and external stakeholders. Finally, when the function of communication is compliance driven, the communication must meet legal and regulatory requirements for notifications of affected individuals, and in certain instances this obligation extends to industry regulators. The legal and regulatory requirements for notifications depend on the cybersecurity incident.

Detection, Analysis, Containment, Eradication, and Recovery

In the detection and analysis phase, what is determined is whether or not an incident has occurred. Once a cybersecurity incident is detected, the cybersecurity incidents are evaluated, and decisions are made on how the cybersecurity incidents need to be addressed. The incident response plan should thus include the manner in which the organization/agency will respond to a cybersecurity incident. This plan should consider the ways in which the response to the incident will minimize damage and reduce the costs associated with response to and recovery from a cybersecurity incident and the procedures that will be followed to communicate the cybersecurity incident to relevant internal and external stakeholders (Cyber Security Coalition 2015; Cichonski et al. 2012). The response to incidents includes the specific procedures that should be followed to contain a cybersecurity event (i.e., the identification and isolation of the system impacted by a cybersecurity threat and/or the area targeted by the threat to prevent harm/damage to other areas) and to investigate and/or to resolve the cybersecurity incident (Cyber Security Coalition 2015; Cichonski et al. 2012). Particularly, this part of incident response involves the containment, eradication, forensic analysis of, and recovery from the cybersecurity incident, wherever appropriate (Cichonski et al. 2012).

There are two dilemmas associated with incident response: recover quickly or gather evidence (Cyber Security Coalition 2015). The first dilemma is whether to disconnect the network or shut down systems in order to facilitate a faster recovery. This approach is not conducive to an investigation of a cybersecurity incident. On the positive side, this approach enables a faster recovery from an incident (although this depends on the type of cybersecurity incident and whether or not full or partial recovery is possible) and enables a fast response, which minimizes the amount of time an attacker has to compromised the system, corrupt information, or steal data. On the negative side, this approach will alert the perpetrator of the cyberintrusion or cyberattack of the discovery of the incident. Also, if this approach is followed, then it is likely that vital information will be missed and lost, which means that a similar incident may be likely experienced in the future. The second dilemma involves the approach of monitoring the cyberintrusion and focusing on *digital forensics* (i.e., "a branch of forensic science that focuses on criminal procedure law and evidence as applied to computers and related devices,"

Maras 2014a, p. 29) applications in order to gather information about the cybersecurity incident. This approach is much more thorough than the one previously discussed and enables the identification of the root causes of the issue and the manner in which these issues can be resolved. This type of approach is essential for gathering evidence that could be used in a court of law (Maras 2014a). This approach, however, will delay recovery from the cybersecurity incident.

In this phase, the acquisition, preservation, securing, and documentation of evidence occur (Maras 2014a). During the investigation phase, a determination is made of the root cause of the cybersecurity incident and the magnitude of its impact. Identifying the root cause of the incident is essential to the eradication and cleanup process that follows a cybersecurity incident. This phase involves the removal of all artifacts (i.e., digital footprints) that have been left behind by the perpetrator including malware, as well as dealing with vulnerabilities identified during or after the cybersecurity incident. The severity of the cybersecurity incidents will also dictate the response. It may be necessary to quickly respond to the cybersecurity incident to prevent the harm caused to systems, devices, and networks within an organization/agency (Maras 2014a). Overall, before cybersecurity incidents, the impacts of various containment and eradication strategies should be identified, particularly the impact of these strategies on the efficacy and efficiency of operations of organizations/agencies (Kent et al. 2006).

The recovery phase includes an analysis of the cybersecurity incident and response to the incident in order to determine the procedural and policy implications of the incident and to gather information about the particulars of the cybersecurity incident, as well as to identify lessons learned with the intention of incorporating them into future activities and training (Cichonski et al. 2012; Maras 2016). An essential element in the recovery process is communications – this helps repair the reputation of the organization/agency after an incident, if this reputation was damaged due to the extent of the cybersecurity breach and the handling of the breach by the organization. Redundancy features, such as system backups, are also essential components for recovery.

Recovery planning should include the processes and procedures that are implemented to maintain operations and ensure the restoration of any assets or systems that were affected by cybersecurity incidents to an operationally ready and/or pre-incident state (Cichonski et al. 2012; Maras 2014a, 2016; Cyber Security Coalition 2015). Remediation involves repairing all affected systems and performing analyses to determine that the cybersecurity threat has indeed been contained (Cyber Security Coalition 2015). Within this phase all relevant stakeholders and individuals who are part of the incident response should be instructed on what to do to repair the harm caused, and/or individuals who were targeted in the cybersecurity incident should be instructed on what to do to protect themselves against further incidents. The restoration activities should also be coordinated with all relevant internal and external stakeholders.

Lessons Learned

The last stage involves lessons learned, which is more than determining what actually happened in the cybersecurity incident and also involves figuring out ways to improve existing processes and to better defend and protect systems, network, services, and data from future cybersecurity incidents. The lessons learned should include a detailed description of what happened; when the incident occurred; how well the incident was handled; whether procedures were followed; assessment of the adequacy of these procedures to deal with the cybersecurity incident; any actions that may have hindered or forestalled recovery; any actions that might be taken for future incidents that were not taken for the current cybersecurity incident; the measures that can and have been implemented to prevent future similar incidents or at the very least mitigate future similar incidents; and any other tools or other resources needed to detect, analyze, mitigate, and prevent future cybersecurity incidents (Cichonski et al. 2012; Maras 2014b). A post-

incident review is essential because it provides the details about an incident and any actual impacts of the incident.

Conclusion

Ultimately, the incident response plan should be detailed, updated regularly, and tested to ensure that the cybersecurity incident handling processes identified within the plan are viable. This updating is also needed to ensure that the plan is designed to provide guidance on new and emerging cybersecurity threats and new policies and procedures with respect to incident response.

Cross-References

- ▶ Cybersecurity: Policy
- ▶ Cybersecurity: Preparedness
- ▶ Investigations: Cybercrimes

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology. NIST special publication 800-61 Revision 2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Cyber Security Coalition. (2015). Cyber security incident management guide. https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide for integrating forensic techniques into incident response. NIST special publication 800-86. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook CMU/SEI-2003-HB-001. https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf.

Maras, M.-H. (2014a). *Computer forensics: Cybercriminals, laws and evidence* (2nd ed.). Burlington: Jones and Bartlett.

Maras, M.-H. (2014b). *Transnational security*. Boca Raton, FL: CRC Press.

Maras, M.-H. (2016). *Cybercriminology*. New York: Oxford University Press.

Newhouse W., Keith, S. Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. NIST special publication 800-181. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Young, S. (2013). Incident response and SCADA. In R. Radvanovsky & J. Brodsky (Eds.), *Handbook of SCADA/control systems security*. Boca Raton: CRC Press.

Further Reading

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide for integrating forensic techniques into incident response. NIST special publication 800-86. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

C

Cybersecurity: Policy

Alex Chung[1], Sneha Dawda[1], Atif Hussain[2], Siraj Ahmed Shaikh[2] and Madeline Carr[1]
[1]Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), University College London, London, UK
[2]Systems Security Group, Institute for Future Transport and Cities (FTC), Coventry University, Coventry, UK

Keywords

Adaptive policymaking (APM) · Agile governance · Attribution · Budapest Convention · Critical infrastructure · Cyber · Cyberattack · Cybercrime · Cybersecurity · European Union (EU) · Evidence-based policymaking · Geopolitics · Incident response · International relations · Mutual legal assistance treaty (MLAT) · UK National Cyber Security Centre (NCSC) · National cyber security strategy (NCSS) · US National Cyber Strategy (NCS) · US National Security Strategy (NSS) · Polycentric governance · Public policy · Public-private partnership · Socio-technical · Tallinn Manual · United Kingdom (UK) · United Nations (UN) · United States (USA) · Wicked problem

Definition

Cybersecurity policy refers to a course of action adopted by a state, an organization, or a set of actors with the aim of ensuring cybersecurity and/or digital competitiveness as well as defining the individual and collective responsibilities in pursuit of that goal.

Introduction: What Is Cybersecurity Policy and Why Does It Matter?

Cybersecurity policy refers to a course of action adopted by a state, an organization, or a set of actors with the aim of ensuring cybersecurity and/or digital competitiveness as well as defining the individual and collective responsibilities in pursuit of that goal. Broadly conceived, this area of public policy concerns complex, multifaceted, and dynamic security and business innovation related to information and communications technology (ICT). Cybersecurity policymaking includes legal, regulatory, technical, organizational, behavioral, international, and other capacity-building areas. Policy dimensions attached to these include information security, network security, cybercrime, and cyber conflict.

Cybersecurity policy can be formulated and implemented domestically at different levels of government or at the international level. The policy scope can range from short- to longer-term objectives and has implications for a wide range of societal actors. Effective cybersecurity policy can have consequences for public safety, national security, citizens' well-being, and economic prosperity. As became clear in the wake of the alleged interference in the 2016 US elections, it can even have implications for the health and sustainability of democratic processes.

Some governments produce clearly articulated cybersecurity policy goals, objectives, and strategies which are publicly accessible. Others struggle to develop these due to a lack of capacity or the weight of more immediately pressing problems. Still other governments develop cybersecurity policies but choose not to share them with their own citizens or other governments. Therefore, the study of cybersecurity policy often focuses on those countries that do publish their plans – countries like (but certainly not limited to) the United States (USA), Japan, Australia, Norway, France, Germany, Canada, and the United Kingdom (UK; see http://ccdcoe.org for a list of published national cybersecurity strategy documents).

In these countries, cybersecurity policy tends to coalesce around the promotion of the national interest with security, defense, and the resilience of the private sector most often prioritized in government agendas. Specific issues tend to include the protection of critical national infrastructure and critical information infrastructure, continued industrial and business growth and innovation, the prevention of fraud, cybercrime, and child sexual exploitation, as well as defending against state-sponsored misinformation propaganda and other state-sponsored malicious cyber activities.

In a world where the pace of digitalization is accelerating, a comprehensive and well-thought-out cybersecurity policy that is based on defined legal and regulatory frameworks is understood to be a cornerstone of prosperous and proper functioning societies. However, identifying what exactly constitutes "good" cybersecurity policy is difficult for a number of reasons. This is not a mature area of policymaking and there are some factors which make it particularly challenging. These include coordination problems of any diverse policy issue across portfolios, the close interdependence of government with the private sector for pursuing cybersecurity, and the challenges of jurisdiction which sometimes defy cyber incidents.

What Factors Complicate Cybersecurity Policy?

Coordination Problems

Cybersecurity in one form or another can now be found in many (if not most) policy portfolios. In a health portfolio, cybersecurity might relate to the security of personal health records or to the safety of Internet-enabled equipment and personal health devices. Cybersecurity has implications for

international trade as governments vie for lucrative contracts for their own indigenous firms while, at the same time, a business development portfolio may be working to attract large multinational corporations by offering tax relief in order to stimulate local jobs. Cybersecurity is central to law enforcement, defense, and intelligence communities as it is seen as an important element of national security. It is not surprising that with the breadth of issues, interests, objectives, and goals among these and the many other policy portfolios engaging with cybersecurity, coordination can be extremely difficult.

Policy areas that pertain to national emergency and incident response cover a vast array of public and private cybersecurity spheres. Some of the relevant sectors include telecommunications, electrical and nuclear power, transportation, energy pipelines, weapons systems, refineries, financial networks, and healthcare systems. The effectiveness of policy is dependent upon the joint implementation between the government and the private sector. National technical authorities such as the National Cyber Security Centre (NCSC) in the UK and the National Cybersecurity and Communications Integration Center (NCCIC) in the USA have been established to monitor, collect, and share information with their partner organizations. These coordination efforts have proven particularly challenging during emergency situations due to the complexities of multi-stakeholder involvement. To communicate information in a timely and accurate way, it is important to know where clear lines of communications lie between the private sector and government agencies responsible for intelligence, defense and security, law enforcement, and commerce and finance.

Clearly, a high level of coordination is required to increase the overall effectiveness of national and local policies. At the same time, too much centralized control raises concerns about a lack of flexibility and independent thinking – both qualities understood to be important in cybersecurity. Consequently, there is a persistent tension in many countries about how to balance coordination and autonomy in portfolio-level decision-making. This leads to questions about the role that public-private partnerships (PPP) play in national cybersecurity policy implementation. This concept has been growing in prominence in recent years and now features as the centerpiece in the strategies of many developed countries.

Public-Private Partnership

Critical national infrastructures of developed countries have experienced a progressive shift toward a market-led management approach since the turn of the century. In the context of an overall shift to small government, the control over ICT estates as well as related knowledge, skills, and expertise have increasingly been relegated to the private sector rather than being retained by national governments. As a result, there has been a high level of outsourcing of responsibility, ownership, and capability to private entities. Governments regard this as a means of relieving financial burdens and remaining up to date in a rapidly evolving technological landscape. As a consequence, the PPP has now become a key mechanism for the mitigation of cybersecurity threats. Many states now rely on PPPs as part of their policy implementation plan (Carr 2016a).

PPPs are important to national cybersecurity policy for a number of reasons. In the USA, for example, over 85% of national critical infrastructure is in private hands. While there is excellence in the military and intelligence communities, commercially available ICT solutions mostly come from the private sector. Governments have an incentive to stimulate and support private sector growth and then draw on its expertise when required. While there are many reasons why the PPP is an important element of national cybersecurity policy planning and implementation, these arrangements are not without problems (ibid.).

Several types of specific PPP arrangements have been identified and classified. These include the dichotomy of horizontal, consensual decision-making partnerships which displays the true nature of PPP versus hierarchical relationships with unipolar power asymmetry. Other PPP arrangements include *partnership as management reform* through the relinquishing of state authority and capability, to *partnership as power sharing*

which entails information sharing rather than responsibility sharing. Clearly articulated (and contracted) PPPs can be very effective, but NCSSs often refer to this in an amorphous way, "we are bound together in cyberspace" (Osborne 2015) type of arrangement which fails to specify lines of responsibility and liability for national security issues. As a core responsibility of the government, national security should not be outsourced in principle, especially when the private sector has no interest in accepting it in practice.

In order for PPP to work to maximum advantage, competing agendas between the government and multinationals who own and who wield significant influence over national security concerns need to be spelled out in the PPPs' design. The distinction between the government's duty to protect national security as a necessary public "good" and profit as the ultimate end for companies needs to be explicit for the middle ground to emerge. To aid this, a shift is required from the normative and "new management" language, which obfuscates a dysfunctional partnership, to a clear language that acknowledges PPP's weaknesses.

Jurisdiction and Speed

Another set of coordination challenges that complicates cybersecurity policy concerns law enforcement investigatory capacity in response to cyber incidents. Unlike crime in the physical world, cybercrime's unique extraterritorial qualities transcend geographical boundaries. The invisible and nonlocal nature of cyberattacks creates obstacles for the authorities to quickly and effectively investigate and apprehend perpetrators.

The sheer volume and scale of potential mass targets for malicious cyber actors render conventional policing strategies ineffective. Police remit in this area includes the investigation of cyber-enabled crimes such as online fraud and child sexual exploitation imagery but also cyber-dependent crimes that incapacitate network systems such as distributed denial-of-service (DDoS) and ransomware. From personal networked devices to commercially sensitive information and from state secrets to critical national infrastructure systems, the expansive coverage of vulnerable digital assets overstretches policing resources. The blurred boundaries between national cybersecurity concerns and civilian targets, due to ever-increasing digital connectedness, also blur responsibilities.

In general, three characteristics of the virtual domain make cyber investigations extremely demanding: actor's anonymity, speed of activity, and multistage action across jurisdictions (BIICL 2014). Rid and Buchanan (2015, pp. 24–25) provide four categories in their explanation of how the speed and phasing of cyberattacks complicate an investigation. A *direct and immediate* attack can reduce uptime of servers, availability of files, or integrity of data and hardware; a *direct and delayed* attack can manipulate critical network systems to stress their components and result in physical breakdown. An *indirect and immediate* attack can cause reputation damage or loss of confidentiality through file leakage; an *indirect and delayed* attack can involve intellectual property theft which may be used to illegally gain a firm's competitiveness.

In addition, cyber attribution is an extremely difficult, if not impossible, exercise. Computer network systems allow criminals to not only conceal their tracks but also to mislead by falsifying the origin of the attack. Digital forensic evidence in this respect resists any attempts by the investigator to accurately identifying malicious actors. Bartholomew and Gurrero-Saade (2016) contend that there will never be a solid enough attribution claim to convince everyone but only multiple indicators that may lead to an educated determination as to the trustworthiness of a claim. Without the ability to attribute attacks with sufficient certainty, authorities cannot take appropriate remedial and deterrent actions (or retaliatory measures) in suspected state-sponsored attacks (ibid.).

Across jurisdictions both within and beyond a nation's borders, network infrastructure and digital connectivity can differ greatly. This creates varying levels of needs and interests for security due to an uneven distribution in the level of risks and attacks, which in turn leads to different levels of preparedness, amount of resources allocated to

law enforcement, and governance methods. Although Western countries have been working on fostering the right environment and processes and enabling cooperation and collaboration on cybersecurity policy, which is discussed below, these issues remain inherently difficult to resolve.

How Is Cybersecurity Policy Implemented?

While the governance approach for dealing with policy issues is distinct for every government, an increase in the use of a polycentric mode of governance has been observed worldwide. Such governance structure involves multiple centers and levels of decision-making within the policy community (Ostrom et al. 1961). The following discussion exemplifies the profound coordination challenges illustrated above by selectively focusing on three examples of cybersecurity policies in the USA, the UK, and internationally. It looks at some key factors affecting cybersecurity policy within the context of incident response and management. These include determining where responsibility lies and how it is delineated within PPPs, which key actors take the lead in creating and implementing cybersecurity strategies, and what are the institutional remits of the relevant agencies as well as how their work intersects to promote effective collaboration.

In the USA

In 2003, the USA was the first state to develop a national cyber security strategy (NCSS) titled the National Strategy to Secure Cyberspace and has invested heavily in policy innovation and coordination. The US National Cyber Strategy 2018 (NCS) and National Security Strategy 2017 (NSS) contain prescriptive provisions salient to cybersecurity. At the core of the policy ecosystem sits the Department of Homeland Security (DHS). The DHS conducts high-impact cybercrime investigations alongside other federal agencies. It also attempts to work with federal civilian departments and agencies to promote the adoption of common policies and to share cyber response best practices and tools. This includes the US Computer Emergency Readiness Team (US-CERT) which sits within the NCCIC, a round-the-clock awareness and incident response management center for integrated cross-government communication.

In addition, the DHS also promotes cybersecurity on several fronts through engagements with its partnering organizations. These include public awareness campaigns, cyber insurance market, research and development, jobs and training, and skills and education. Apart from the DHS, a number of US government bodies are also charged with mandates relevant to cybersecurity policymaking. For instance, the Departments of Commerce (USDC), Defense (DOD), Treasury (USDT), Energy (DoE), Health and Human Services (HHS), and Justice (DoJ) all work in conjunction with the DHS to safeguard different areas of the US cybersecurity ecosystem by jointly executing policy plans.

Notwithstanding the roles government actors take on to shape and direct cybersecurity policy at the federal level, implementation is far from a straightforward process. While the DHS's coordination role is meant to be supported by a wide range of public and private partners who are operators and co-owners of most of the government critical national infrastructures, policy delivery and outcome are often contested. Although PPP cooperation and collaboration are vital to the implementation of cybersecurity policies (which includes the NCS 2018 and NSS 2017) at the federal level, nonfederal influences are seriously impeding the effective coordination of critical infrastructure policies that aim to protect national security and facilitate cyber risk communications.

The decentralized US federalism system gives rise to simultaneous decision-making and guarding of assets and rights by different institutional actors. For instance, the US Congress, state and local governments, and private companies may choose not to share information with the federal government or adhere to federal level cyber risk guidance if doing so conflicts with their economic interests (Mussington 2018). These obstacles present significant challenges to the country's ability to carry out and maintain coherent cybersecurity policies and operational

response structures that ought to align with executive orders and legislation.

In the UK

As one of the most digitally ambitious countries in Europe, the UK's stated goal is to be "the safest place to live and do business online" (NCSS 2016–2021). Since 2011, cybersecurity has been nominated as a "Tier 1" threat to UK national security (NCSS 2011–2016). The UK has the largest digital economy of the G20, which accounts for 12.4% of the country's GDP, more than double that of the US at 5.4% (techUK 2015). Substantial resources and efforts are allocated by the UK government to ensure that the country's capabilities are at the forefront of this field.

The policy terrain of UK cybersecurity is centrally administered and funded through the Cabinet Office. Similar to the USA and other developed countries, the UK relies on the national cyber security strategy 2016–2021 (NCSS) as the overarching policy document that sets out the strategic direction of, and approach to, ensuring cybersecurity. For the years 2016–2021, the Cabinet Office oversees a budget of £1.9 billion to support the delivery of the NCSS, though they provide minimal top-down operational directives to ministerial departments involved this area.

Remaining behind the scenes, the Government Communications Headquarters (GCHQ) is the primary player leading the effort to ensure the cybersecurity of national information network and communications systems. As the technical authority within the government and the public-facing organization under the GCHQ, the NCSC supports, implements, and coordinates top-level policies. The incident response management team within the NCSC is responsible for assessing and responding to emerging incidents. If the crisis is deemed to pose an immediate threat or a rapidly escalating threat to national security, a Cabinet Office Briefing Room (COBR) meeting is convened where actors such as the National Crime Agency (NCA) may take part in a law enforcement and investigatory capacity. During emergency situations, the central government (HMG) takes action with the assistance of the NCSC to provide points of effective coordination that quickly work to deploy defensive (and offensive) measures against adversaries.

Compared to the USA, the implementation and delivery of the NCSS in the UK are functionally more distributed among HMG ministerial departments, the lead charge for which resides with the Home Office and the Department of Digital, Culture, Media and Sports (DCMS). The former is tasked with operational and strategic foci on cybercrime and cyber threats, while the latter is mandated with cyber growth, innovation, and security. Akin to the USA, the challenge of delivering national policy objectives means public and private institutions are required necessarily to work collaboratively across government and industry sectors.

Internationally

Instead of a single policy framework, the international policy landscape consists of multilateral efforts to jointly agree on rules and harmonize national laws. These comprise of clusters of binding and non-binding instruments reached by states sometimes with the help of international organizations. Binding instruments include conventions, directives, and regulations. Non-binding instruments include declarations, recommendations, and guidelines. Intergovernmental and supranational entities also work together to facilitate the implementation process in the name of global order and security, but mixed results have been obtained so far.

Launched in 2001 and came into force that year, the Convention on Cybercrime of the Council of Europe (Budapest Convention) is the first binding international treaty on crimes committed via the Internet and computer networks. Developed in consultation with the USA, Canada, Japan, and South Africa, it is open to signature by any state and at the time of writing had been ratified by 61 states. To ratify the treaty, states are required to outlaw five actions and authorize their domestic law enforcement agencies to investigate them: unauthorized access, unauthorized interception, data interference, system interference, and misuse of devices (Carr 2016b).

Predominantly an instrument for aligning states' criminal codes to facilitate faster and

more effective cooperation between law enforcement bodies, its uptake has been slow and limited mainly due to technical capability, legal factors, and a lack of political will. The addition of new protocols since 2006 has also led to widespread disagreement among states over the value of their inclusion due to inconsistencies with the public policies and security priorities of states (ibid.). The main legal mechanism upon which treaties such as the Budapest Convention can rely for cross-jurisdictional law enforcement is the mutual legal assistance treaties. Signatories of MLATs have an obligation to reciprocate in all types of criminal investigations and prosecutions Including those with a cyber dimension. Together, MLATs and the Budapest Convention significantly minimize barriers to international cooperation in the enforcement of rules and regulations stemming from cybersecurity policies.

While intergovernmental cybersecurity framework developments can be traced back to the 1990s, there has been a strong push for new policies since the early 2010s due to the novel forms of insecurity and threats that are arising in cyberspace. The "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" contains a comprehensive analysis of how existing international law applies to cyberspace, based on the first 2013 edition. Authored by 19 international law experts led by the North Atlantic Treaty Organization (NATO), the manual's intended audience is global policymakers. According to the authors, its main contributions are that it captures the disagreements between countries on issues of cyber conflict and highlights the need to move away from an offensive posture in cyberspace to a defensive one. It acknowledges, for the first time, the lack of understanding of legal gray areas in cyberspace which creates contentions in the interpretation and application of international law (Ansley 2017).

At the UN level, states have worked together through the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) to negotiate some common understanding and agreement about responsible state behavior in cyberspace. In 2012, all participating states (including Russia, China, and the USA) agreed that international law does apply in cyberspace. Exactly *how* it applies has been the source of ongoing debate. In 2016, the UN GGE produced a consensus report on 11 proposed "norms" of responsible state behavior, but the subsequent meeting in 2017 was dominated by deeply divergent views. The controversies surrounding the politicization of the International Telecommunication Union (ITU) are other examples, where states' different political and belief systems in the amount of control exerted over the Internet have led to the creation of internal factions which have marred its governance effort. Moreover, geopolitical rivalry is reflected in the trend toward regionalism, which impedes wider international cooperation. Different views on cyberspace governance and cyber norms are manifested in the policy stance of regional security groupings.

Notably, the Shanghai Cooperation Organisation (SCO) established in 2001 – comprised of - China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan – emphasized the importance of cyber sovereignty and the creation of a new cybercrime treaty in addition to the Budapest Convention. European Union (EU)-led frameworks such as the Network and Information Security Directive (NISD) and the General Data Protection Regulation (GDPR) tend to focus on self-regulation and compliance measures aimed at managing unavoidable cyber risks and incidents. Despite high-level dialogues between the USA, the UK, the EU member states, Russia, and China on these issues, common ground has not been reached.

Future Thinking

In the twenty-first century, the pervasiveness of software and communications systems allows cyber insecurity to permeate through every facet of citizens' lives (Tanczer et al. 2018). This presents tremendous challenges to policymaking due to the myriad of ways in which it poses potential and real harm to public interest and safety. Policymakers need to make informed decisions based on accurate assessment of the risks,

vulnerabilities, threats, and harm emanating from cybersecurity ecosystem. Yet, they are struggling to achieve this in a cohesive, joined-up way because the cyber domain is a highly dispersed issue with complex interdependencies across portfolios and it is in constant flux.

This combination of two factors produces what are referred to as "wicked problems," and they render policymaking especially challenging. These kinds of "wicked problems" need to be tackled through cross-governmental departments and intergovernmental agencies that have coexisting roles and overlapping functions. The coordination of collaborative efforts to counter these policy issues from multiple centers and levels of a policy network simultaneously, as illustrated in the examples of the USA and the UK, are key organizational features of a polycentric governance structure.

Further, adaptive policymaking (APM) and agile governance have also been on the rise globally, which are now reflected in various national cybersecurity strategies. Agile governance entails adaptive, inclusive, and sustainable policymaking that accounts for not only input from the government but emphasizes collaborative efforts by multi-stakeholders. APM explicitly accounts for deep uncertainties prompted by the speed with which technologies evolve, in contrast to the "classical approach" such as evidence-based policymaking (Haasnoot et al. 2013). APM incorporates a strategic vision and framework from which policies are derived to prepare for negative eventualities while being sufficiently flexible and dynamic to meet changing circumstances through short-term actions (Tanczer et al. 2018).

While the UK and the USA have not clarified the methodological approach behind the design, formulation, and implementation of their NCSSs, agile governance and APM models have come to be recognized as an important tool by the government, industry, and academia of the respective countries (Parcell and Holden 2013). Research on cutting-edge tools and decision-making frameworks that focus on robust evidence uptake and rigorous evidence evaluation is currently being developed to assist the policy process (Hussain et al. 2018).

In the UK, collaborative projects in partnership with government bodies such as the Cabinet Office, the Department of Work and Pensions, the Department of Health, the Ministry of Justice, and the Ministry of Defense are under way to investigate new ways of developing and incorporating agile principles in their policy work. In the USA, organizations such as NIST in the Department of Commerce, American Institute of Aeronautics and Astronautics (AIAA), and federal government infrastructure suppliers are employing an adaptive approach to policy implementation at the federal level.

These approaches are further encouraged for countries working toward common international digital development goals such as the United Nations Sustainable Development Goals. A gradual shift toward an open and inclusive model of multi-stakeholderism is advocated to account for the varied stages of digitalization of each country (Clemente 2013). Despite ongoing development in these areas, much work remains ahead. Commentators have been calling for further research into innovative APM and agile governance models on both national and international fronts and to implement their application more widely and effectively in the realm of digital policymaking.

Conclusion

The complexities of cybersecurity policy are shown through the coordination challenges, PPP obscurities, and jurisdictional issues facing the national and international policy communities. The cyber domain is throwing up uncertainties around issues of national security and national interest, which make it difficult for policy actors to make informed decisions on domestic matters or reach consensus on international concerns. These problems become particularly pronounced when decisive action is needed to respond to cybersecurity incidents and emergencies.

Although governments and private entities have devoted significant resources to better

understand and address the inadequacies, clearer terms of reference are required for effective collaboration in the policy process, and wider international cooperation is needed to resolve geopolitical roadblocks and impasse. To this end, polycentric governance appears to be the preferred approach in the USA and the UK based on how policy design and implementation are organized between the respective governments and the relevant private sector stakeholders. In recent years, research into different modes of agile governance and APM has made headway in addressing the limitations inherent to this socio-technical area of policymaking. Continued refinement of research in the areas of decision-making processes and evidence evaluation frameworks holds promise for a future that is better equipped to deal with the challenges posed by cybersecurity policymaking.

Cross-References

- Big Data
- Criminals: Cybercriminals
- Critical Infrastructure: Critical Manufacturing Sector
- Critical Infrastructure: Transportation Systems
- Data Protection
- Emergency Management: Recent Incidents That Contributed to Changes in Emergency Management Legislation and Procedures
- Industrial Control System
- Insider Threat
- Internet (Deep and Dark Web)
- Internet of Things
- Intrusion Detection Systems
- Public-Private Partnerships: Port Security

References

Ansley, R. (2017, February 15). Tallinn manual 2.0: Defending Cyberspace. *Atlantic Council Blog*.

Bartholomew, B., & Gurrero-Saade, J. A. (2016). Wave your false flags! Deception tactics muddying attribution in targeted attacks. In *Virus bulletin conference*, October.

BIICL. (2014, October 9). State responsibility for Cyber operations: International law issues: Event report. British Institute of International and Comparative Law.

Carr, M. (2016a). Public-private partnerships in national cyber security strategies. *International Affairs, 92*(1), 43–62.

Carr, M. (2016b). Crossed wires: International cooperation on Cyber security. *Journal of International Affairs, 2015/2016*(2), 1–2.

Clemente, D. (2013). Adaptive internet governance: Persuading the Swing States. Internet Governance Papers, No. 5, October.

Haasnoot, M., Kwakkel, J. H., Walker, W. E., & ter Maat, J. (2013). Dynamic adaptive policy pathways: A method for crafting robust decisions for a deeply uncertain world. *Global Environmental Change, 23*(2), 485–498.

Hussain, A., Shaikh, S. A., Chung, A., Dawda, S., & Carr, M. (2018). An evidence quality assessment model for cybersecurity policymaking. In *Technical proceedings: International Federation for Information Processing (IFIP) Conference*, 13 March, Arlington.

Mussington, D. (2018). Governing Cyber Security in Canada, Australia and the United States. In C. Leuprect & S. MacLellan (Eds.), *Centre for International Governance Innovation*: Special Report, April.

Osborne, G. (2015). Chancellor's speech to GCHQ on Cyber Security. *UK HM Treasury online*.

Ostrom, V., Tiebour, C. M., & Warren, R. (1961). The organization of government in metropolitan areas: A theoretical inquiry. *American Political Science Review, 55*(4), 831–842.

Parcell, J., & Holden, S. H. (2013). Agile policy development for digital government: An exploratory case study. In *Conference: Proceedings of the 14th annual international conference on digital government research*.

Rid, T., & Buchanan, T. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1/2), 4–37.

Tanczer, L., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2018). The United Kingdom's emerging internet of things (IoT) policy landscape. In R. Ellis & V. Mohan (Ed.), *Rewired: Cybersecurity governance.* Hoboken: Wiley.

techUK. (2015). UK's digital economy is world leading in terms of proportion of GDP. 1 May.

Further Reading

Her Majesty's Government. (2016). National Cyber security strategy 2016–2021 (cited as NCSS).

NCS. (2018). National Cyber strategy of the United States of America 'National Cyber Strategy of the United States of America.' The White House, Washington, DC, September.

NSS. (2017). National Security strategy of the United States of America. The White House, Washington, DC, December.

Cybersecurity: Practice

George Grispos
School of Interdisciplinary Informatics,
University of Nebraska Omaha,
Omaha, NE, USA

Keywords
Cybersecurity · Best practices · Standards · Policies · Guidelines

Definition

Cybersecurity involves the application and management of techniques with the aim of protecting the confidentiality, integrity, and availability of information and information assets in cyberspace.

Introduction

The widespread use of electronic information processing coupled with the emergence of business conducted through the Internet has fueled the need for organizations to protect proprietary and customer information from malicious cyber actors and nations (Grispos et al. 2017). As a result, many organizations have recognized the importance of implementing effective cybersecurity practices. According to the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), cybersecurity encompasses the preservation of confidentiality, integrity, and availability of information in cyberspace (International Organization for Standardization/International Electrotechnical Commission 2012). Confidentiality refers to "the protection of sensitive information from unauthorized disclosure" (Peltier 2013). Integrity is defined as "the accuracy, completeness, and validity of information in accordance with business values and expectations" (Peltier 2013). Availability relates to "information being available when required by the business process now and in the future" (Peltier 2013). Collectively, *confidentiality*, *integrity*, and *availability* are referred to as the CIA triad. An organization's cybersecurity objectives should be to protect the confidentiality, integrity, and availability of information and information assets within its distinct cyberspace. Various approaches can be taken to achieve this objective including through the implementation of security controls; enforcing security polices, standards, and guidelines; using risk management approaches; as well as, education and training initiatives. These approaches have existed and matured over several decades and have been classified in terms of generational waves.

Cybersecurity Waves

As part of a wider analysis into cybersecurity practices within organizations, Von Solms (2000, 2006) separated the evolution of cybersecurity countermeasures within organizations into four generational "waves". The first generation of cybersecurity countermeasures existed up until the early 1980s and can be characterized as the "Technical Wave". In this generation, cybersecurity countermeasures focused on mainframes and data centers, where solutions focused on enhancing the cybersecurity of the operating system through access control lists, user IDs, and the use of passwords. In addition, physical security barriers were also the norm. The second generation of countermeasures (the "Management Wave"), lasted from the early 1980s to the mid-1990s and emerged with management within organizations realizing that security was no longer just a technical issue. Hence, organizations needed to develop cybersecurity policies and procedures and integrate managers and executives in the security decision-making process. The third generation of countermeasures (the "Institutional Wave") started in the mid-1990s and continued into the early 2000s. This wave is characterized by the demand for organizations to implement cybersecurity standards and best practices. As a result, many organizations looked to implement standards and best practices such as the International Organization for Standardization/

International Electrotechnical Commission (ISO/IEC) 27001 standard. The fourth-generation wave (Von Solms 2006) (the "Information Security Governance Wave") developed at the turn of the millennium and emerged as a result of new legal and regulatory requirements dictating that organizations implement cybersecurity policies and processes to protect information and information systems. Therefore, this wave defines that an organization's security governance is included and part of its overall corporate governance posture.

Cybersecurity Programs

In an effort to address their cybersecurity objectives, many organizations have chosen to implement *cybersecurity programs (Grispos* et al. 2013*)*. The primary objective of a cybersecurity program is to protect the CIA triad while also ensuring that any legal and regulatory requirements are also fulfilled. Several organizations and government agencies, such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), and the Internet Engineering Task Force (IETF), have published frameworks, processes, and best practice guidelines describing how organizations can reduce cybersecurity risk and enhance their security posture.

The NIST Cybersecurity Framework

In February 2013, the President of the United States issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity. In particular, the Executive Order called for the development of a risk-based Cybersecurity Framework including industry standards and best practices to help organizations manage and mitigate cybersecurity risks. NIST answered this call to arms by publishing in 2014 a document called the "Framework for Improving Critical Infrastructure Cybersecurity," which has since been updated in 2018 (National Institute of Standards and Technology 2018). To achieve these objectives, NIST have published a series of documents, called Special Publications (SPs), that can be used either collectively or individually to secure information assets. These documents include:

- SP 800–12 provides an overview of cybersecurity security and emphasizes the importance of the cybersecurity controls and the different ways to implement them.
- SP 800–14 describes common security principles that are used and that should be incorporated within a cybersecurity policy. These guidelines can be used to enhance existing policies and develop new policies.
- SP 800–37 provides a risk-based approach called the "Risk Management Framework." The publication provides guidelines on applying the Framework to information systems with the aim of identifying what security controls are needed, how they can be implemented, and how security control effectiveness can be assessed.
- SP 800–53 specifically describes 194 security controls that could be applied to an information system in order to enhance the security and privacy of both the system and the information that can reside within the system itself.

It must be noted that while NIST has developed and published the Framework and SPs with the aim of securing critical infrastructure and federal government information systems, any organization is free to use this approach to establish a minimum security-control baseline within their specific environments (Ross 2007).

ISO/IEC 27000 Family of Standards

The ISO/IEC 27000 family of standards are an alternative set of practices that can be applied to mitigate cybersecurity attacks. The last major revision to these standards was published in 2013. While there are nearly 50 standards in the 27000 family, two main standards called ISO/IEC 27001 and ISO/IEC 27002 are considered the baseline for cybersecurity management. The ISO/IEC 27001 standard specifies how an organization can develop and implement an Information Security Management System (ISMS). An ISMS

is defined as "the policies, procedures, guidelines, associated resources, and activities, collectively managed by an organization, in the pursuit of protecting its information assets" (International Organization for Standardization/International Electrotechnical Commission 2014). Similarly, Eloff and Eloff define an ISMS as "used for establishing and maintaining a secure information environment" (Eloff and Eloff 2003). Regardless, once an organization has met the requirements specified in ISO/IEC 27001, it can become certified following the successful completion of an audit to determine it complies with the standard. The ISO/IEC 27001 standard recommends that organizations use an improvement process such as Plan-Do-Check-Act (PDCA) or Six Sigma's Define, Measure, Analyze, Improve, and Control as a method for designing, implementing, and reviewing an ISMS within their respective organization.

Within the above methods, organizations are required to identify and assess cybersecurity risks and then select appropriate security controls. ISO/IEC 27002 is a standard that provides security control recommendations, which can be used during the initiation, implementation, and maintenance of secure systems. SO/IEC 27002 consists of fourteen security domains, which cover cybersecurity control information including security policies, asset management, human resource security, business continuity management, and operations security (International Organization for Standardization/International Electrotechnical Commission 2013). The idea behind ISO/IEC 27002 is that the security controls can be applied to various organizations, irrespective of type, size, risks, or the threats faced by the organization. Hence, the range of security controls covered in the standard can also provide an organization with some flexibility to adopt only the controls that they require within their distinct environment.

IETF Request for Comments (RFC) 2196

RFC 2196 is a cybersecurity standard, formally called "Site Security," published by the Internet Engineering Task Force (IETF). The standard that was published in 1997 is intended to guide organizations during the development of cybersecurity policies and procedures to protect systems connected on the Internet. While the document might appear outdated, much of the information and practical guidance is still very much relevant to organization trying to secure their information and information assets. A range of cybersecurity subjects are covered in RFC 2196 including Firewall implementation, network security, security incident handling, policy development, and risk management.

Other Cybersecurity Practices

Depending on its type, an organization may decide to implement cybersecurity practices that have been specifically developed for its particular domain. For example, the Payment Card Industry Data Security Standard (PCI-DSS) was developed by a number of major credit card companies. The purpose of PCI-DSS is to provide consistent security controls for organizations around the world that manage, handle, and storage payment card information. At the time of writing, the current version of PCI-DSS (Version 3.2.1) was released in May 2018. Changes are usually made to the standard every 3 years. PCI-DSS specifies twelve requirements, which are organized into six control objectives (PCI Security Standards Council 2018):

1. **Build and Maintain a Secure Network and Systems**

   Requirement 1: Install and maintain a firewall configuration to protect cardholder information.

   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
2. **Protect Cardholder Data**

   Requirement 3: Protect stored cardholder data.

   Requirement 4: Encrypt transmission of cardholder data across open, public networks.
3. **Maintain a Vulnerability Management Program**

   Requirement 5: Protect all systems against malware and regularly update antivirus software or programs.

Requirement 6: Develop and maintain secure systems and applications.

4. **Implement Strong Access Control Measures**
   Requirement 7: Restrict access to cardholder data by business need to know.
   Requirement 8: Identify and authenticate access to system components.
   Requirement 9: Restrict physical access to cardholder data.
5. **Regularly Monitor and Test Networks**
   Requirement 10: Track and monitor all access to network resources and cardholder data.
   Requirement 11: Regularly test security systems and processes.
6. **Maintain an Information Security Policy**
   Requirement 12: Maintain a policy that addresses information security for all personnel.

While PCI-DSS is not legally binding within the European Union, there are some States in the United States of America where specific laws directly refer to PCI-DSS. For example, the State of Washington has incorporated the PCI-DSS standard into state law, which stipulates that compliant organizations are shielded from liability, in the event of a data breach or a security incident (The House of Representatives of the State of Washington 2010).

Another example of cybersecurity practices developed for a specific domain is the requirements described in the "Security Rule" within the Health Insurance Portability and Accountability Act (HIPAA) of 1996. More specifically, the Security Rule establishes cybersecurity standards for healthcare organizations that are legally required to protect electronic Personal Health Information (ePHI). This includes implementing appropriate administrative, physical, and technical security controls that will ensure that confidentiality, integrity, and availability of ePHI is upheld. While HIPAA provides explicit security requirements that must be implemented by healthcare organizations, an organization can select and implement security controls from various sources, including NIST Special Publications and ISO 27002.

Cybersecurity Programs in Practice

While some organizations could be legally required to implement cybersecurity practices, there are other benefits to creating, deploying, and maintaining cybersecurity programs. Siponen and Willison argue that organizations who implement cybersecurity programs can "demonstrate their commitment to secure business practices; apply for security certification, accreditation, or a security-maturity classification attesting to their compliance to a set of rules and practices" (Siponen and Willison 2009). Effectively, implementing cybersecurity programs provides an organization with a baseline for improving its overall cybersecurity management strategy.

Several researchers (Siponen 2006; Siponen and Willison 2009; Wiander 2007) have examined how organizations implement cybersecurity programs and evaluated how these programs impact an organization's wider security posture. Wiander (2007) evaluated how four organizations implemented ISO/IEC 17799 security standard. The results from this analysis showed that implementing cybersecurity programs within these organizations increased the overall understanding of cybersecurity by employees within the organizations (Wiander 2007). However, Wiander also observed that many individuals within these organizations found it difficult to implement the security standard, with the readability of the standard being one of the main problems cited during the study. Siponen (2006) made similar observations and added that many cybersecurity standards are not universally validated because they are based on personal experiences. Hence, Siponen (2006) argues that cybersecurity standards should not be treated as a "gold standard" but rather as a library of material for organizations to enhance their security posture. These concerns were further validated in a later study (Siponen and Willison 2009) when four cybersecurity standards were evaluated in several organizations. Siponen and Willison (2009) argued that when these standards are developed, they do not pay enough attention to the differences between organizations and their differing cybersecurity requirement. For

example, while a larger organization could place equal emphasis on all aspects of information security, a smaller organization might lack the demand for a dedicated security incident management team and place more emphasis on antivirus solutions and firewalls. Hence, there could be cases where some organizations are not in compliance with a particular standard because they lack the resources to segregate security functions (Siponen and Willison 2009).

Conclusions

Addressing cybersecurity effectively is an extremely difficult and complex task. This is because there is no single solution to all of an organization's security challenges. While the threat from malicious actors and nations continues to increase, organizations are under continuous pressure to identify and implement cybersecurity controls to protect company and customer information assets. One solution could involve an organization designing and implementing a cybersecurity program based on cybersecurity best practices proposed by organizations such as NIST, ISO/IEC, and IETF. However, financial constraints often limit the number and type of security controls that can be implemented within an organization. Hence, the best approach to implementing cybersecurity practices is one where an organization takes into consideration its legal and regulatory obligations while balancing the cost of security controls.

Cross-References

► Cybersecurity: Policy

References

Eloff, J. H., & Eloff, M. (2003). *Information security management: A new paradigm.* Paper presented at the Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.

Grispos, G., Glisson, W. B., & Storer, T. (2013). *Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization*. Paper presented at the 21st European Conference on Information Systems, Utrecht.

Grispos, G., Jesús, G-G., Liliana, P., & Bashar N. (2017). Are you ready? Towards the engineering of forensic-ready systems. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, pp. 328–333. IEEE.

International Organization for Standardization/International Electrotechnical Commission (2012). *Information technology – Security techniques – Guidelines for cybersecurity.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

International Organization for Standardization/International Electrotechnical Commission (2013). *Information technology – Security techniques – Code of practice for information security controls*.

International Organization for Standardization/International Electrotechnical Commission (2014). *ISO/IEC 27000 – Information security management systems – Overview and vocabulary.*

National Institute of Standards and Technology (2018). *Framework for improving critical infrastructure cybersecurity.*

PCI Security Standards Council (2018). *Payment Card Industry (PCI) Data Security Standard (DSS), version 3.2.1*.

Peltier, T. R. (2013). *Information security fundamentals*. Boca Raton: CRC Press.

Ross, R. (2007). Managing enterprise security risk with NIST standards. *IEEE Computer, 40*(8), 88–91.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM, 49*(8), 97–100.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

The House of Representatives of the State of Washington (2010). *Financial information security breaches – Credit and debit cards, chapter 151, laws of 2010 – House Bill 1149*.

Von Solms, B. (2000). Information security – The third wave? *Computers & Security, 19*(7), 615–615.

Von Solms, B. (2006). Information security – The fourth wave. *Computers & Security, 25*(3), 165–168.

Wiander, T. (2007). *Implementing the ISO/IEC 17799 standard in practice-findings from small and medium sized software organisations.* Paper presented at the 5th International Conference on Standardization and Innovation in Information Technology, 2007. SIIT 2007.

Further Reading

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy.* Springer. Basingstoke, United Kingdom.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity – How to build a successful cyberdefense program against advanced threats*. New York: Apress.

Cybersecurity: Preparedness

Marie-Helen Maras
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Preparedness · Exercises · Cyber Storm · Red team/blue team

Definition

Cybersecurity preparedness assists public and private sector agencies in being ready for cybersecurity incidents that may occur and are essential for the mitigation of materialized cybersecurity threats.

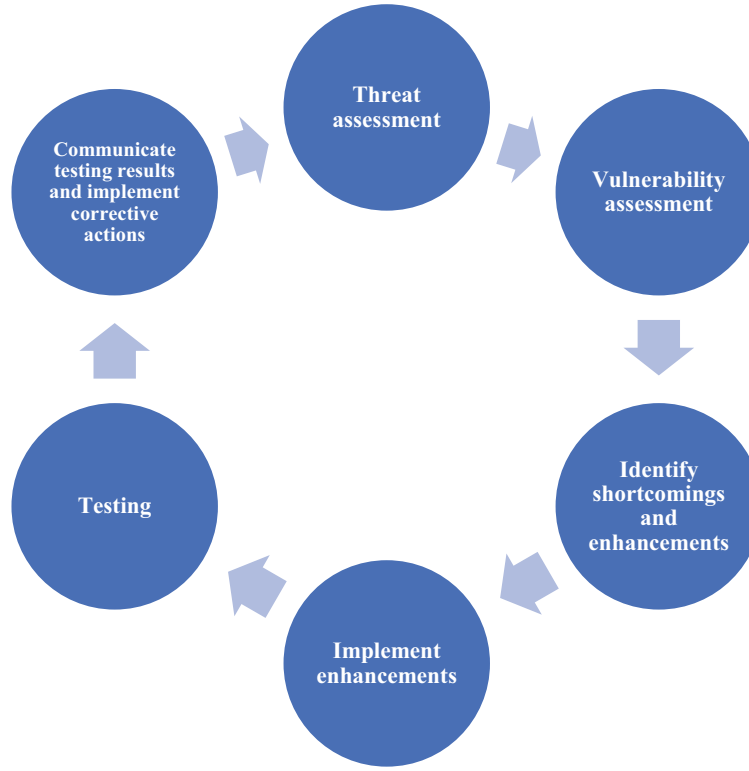
Introduction

Cybersecurity measures have retrospective and prospective capabilities. Retrospectively, these measures seek to respond to incidents while they are occurring or after they have occurred. Generally, this form of cybersecurity seeks to take action or solve something after the fact. Prospectively, these measures seek to mitigate or prevent something from occurring in the future. Cybersecurity measures, therefore, seek to anticipate threats before they materialize, forestall threats, and take action to lessen the impact of a threat once it has materialized. Having incident response plans in place is not all that is needed. These plans need to be viable and useful in the event of cybersecurity incidents to guide individuals involved in incident response on the ways in which to effectively handle a cybersecurity incident. These plans also need to be assessed.

Cybersecurity Preparedness Cycle

The U.S. Department of Homeland Security (2012) defines preparedness as "a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response." Preparedness should thus not be viewed as linear activity but as a cycle (Fig. 1).

The figure in the slide depicts general phases of the preparedness cycle (between agencies and their practices, there may be variation in these phases). The first phase of the cycle is the threat assessment. Threats are circumstances that could cause unintentional and intentional harm. For instance, the hardware of digital technologies can malfunction or be purposely damaged by hackers exploiting firmware vulnerability. The second phase of the preparedness cycle is the vulnerability assessment (i.e., the susceptibility of a device to harm). Vulnerabilities in digital technologies can be found in hardware, software, and system design and configurations or can be external to the digital technologies, whereby the users of technologies may become susceptible to, for example, malware infection by way of their use of these technologies (e.g., using easy to guess passwords, opening email attachments from unknown senders, etc.). The third phase of the preparedness cycle identifies shortcomings of existing cybersecurity measures to deal with the previously identified threats and vulnerabilities (e.g., a lack of intrusion detection systems, inadequate computer-use policies, lack of cybersecurity awareness training for personnel, etc.). After these shortcomings have been identified, enhancements should be identified to deal with these shortcomings. The fourth phase of the preparedness cycle is to implement these proposed enhancements. Some professionals stop here. Stopping at this stage results in the inability to check whether the enhancements implemented are actually designed to deal with the identified threats and vulnerabilities. To determine this, the next stage of the cybersecurity preparedness cycle (the fifth phase) must be completed: the testing phase. In this phase, exercises that include cybersecurity



Cybersecurity: Preparedness, Fig. 1 General phases of the preparedness cycle

simulations (such as simulated threats targeting the vulnerabilities previously identified) are conducted to test the efficacy of the enhancements. The next phase (the sixth phase) involves the reporting and/or communication of the results of the testing and the implementation of corrective actions. Preparedness, however, should not stop there: a reassessment of the cybersecurity threats and vulnerabilities based on these corrective actions should occur.

Cybersecurity Preparedness Exercises

Cybersecurity preparedness and a well-developed and tested incident response plan are essential for the mitigation of materialized cybersecurity threats. Cybersecurity preparedness thus helps reduce adverse impacts from a cyberintrusion. Cybersecurity preparedness exercises are designed to facilitate cooperation and collaboration on responses to hypothetical cybersecurity incidents. Preparedness exercises also assist in improving coordination between internal and external stakeholders during cybersecurity events. Additionally, these exercises enhance awareness and understanding of incident response plans and potential cybersecurity threats and their impact on security. Moreover, these exercises assist in the identification and assessment of cybersecurity incident response capabilities, as well as an evaluation of the sufficiency of existing human and technical resources. These exercises, therefore, can improve response capabilities to real-life events. Furthermore, these exercises enable the evaluation of the incident response plan, identifying any deficiencies in planning and procedures and assessing or validating any modifications that have been made to the plan and procedures.

The scenarios that form the basis of many of these exercises help identify the highest priority issues, the immediate needs of an organization/business, the capabilities to improve the situation following the cybersecurity incident, the available assets to engage in incident response, and unique

and innovative solutions to respond to the incident. Cyber Storm exercises involve and are based on real-world cybersecurity incidents. There have been many iterations of the Cyber Storm exercise (the various Cyber Storm exercises can be found here: CISA 2019a). Each Cyber Storm exercise builds on the previous exercise and the lessons learned from the exercise to create more challenging scenarios for participants. Beyond Cyber Storm, the National Cybersecurity and Communications Integration Center "co-sponsore[s] the Cyber Guard exercise series, the largest tactical-level cyber exercise series in the nation, in cooperation with the U.S. Cyber Command and the Federal Bureau of Investigation" (CISA 2019b).

Types of Preparedness Exercises

Several preparedness exercises can be used to evaluate incident response plans, procedures, and capabilities. These include operations-based and discussion-based exercises (Grance et al. 2006; Dewar 2018; DHS Ready n.d.; NYS-OEM n.d.):

Operations-based exercises. Operations-based exercises are implemented in order to identify and differentiate between relevant stakeholders' roles and responsibilities during incident response and assess existing policies, plans, and procedures. There are several types of these exercises, three of which are functional exercises, full-scale exercises, and drills. *Functional exercises* enable participants to validate an organization's cyber-readiness, as well as existing cyber-incident response plans, by enabling participants in the exercise to perform their duties as prescribed by these plans during a simulated cybersecurity incident (Grance et al. 2006). The activities of participants are driven by the scenario and are not only designed to test the plans and procedures included in the plan but also participants' abilities to execute these plans and procedures. A *full-scale exercise* also enables participants to test and validate an organization's readiness, but this time this exercise is as close to a real-world cybersecurity event as possible. This exercise uses the personnel that would engage in the real-world cybersecurity event and the technical resources (e.g., equipment) they would use if a real-world cybersecurity incident occurred. Full-scale exercises are predominately conducted by government agencies. These exercises can be multiorganization and multijurisdictional and involve both first responders and many other relevant stakeholders in incident response. *Drills* are performed within an organization to systematically test a specific cybersecurity role, function, and/or process of an organization or a single unit or department within an organization.

Discussion-based exercises. As the name implies, discussion-based exercises involve facilitators who ensure objectives of the exercises are met and lead discussions regarding the exercises. The ultimate goal of these exercises is for participants to familiarize themselves with cybersecurity policies, plans, and procedures. Examples of these exercises are seminars, workshops, tabletop exercises, and games (EMI n.d.). *Seminars* include basic training for individuals involved in cybersecurity incident response, as well as other members of the organization. *Workshops* are similar to seminars but often include the creation of some output such as a draft policy or plan. These workshops are designed to familiarize individuals with cybersecurity incident response plans. These workshops are also designed to familiarize all individuals with their roles and responsibilities within these plans. *Tabletop exercises* are discussion-based, whereby facilitators guide the discussions of cybersecurity incident scenarios and participants discuss their roles during cybersecurity incidents and their responses to cybersecurity incidents. The length of tabletop exercises depends on the number of participants, the location of the participants (nationally, internationally, within or outside of one organization/agency, etc.), the type of cybersecurity incidents in the exercise, and the objectives of the exercise. *Games* are based on real-life cybersecurity events (e.g., a worst-case scenario or an anticipation of an evolution of a tactic used by cybercriminals, an evolution of the capabilities of malware, or the exploitation of some new technology by illicit actors in order to cause harm). An example of a wargame, Digital Pearl Harbor, was conducted by

the US Navy War College in 2002 that involved a coordinated and cross critical infrastructure cyber-attack (Wilson, 2003).

Red Team/Blue Team Exercises

Taking a leaf out of the military's playbook, red team and blue team exercises can and have been implemented in private and public sector cybersecurity preparedness (Brangetto et al. 2015; Dewar 2018). The red team/blue team exercise, originally used in the US military in war gaming, enables the application of information learned in trainings and classrooms to hypothetically create a cybersecurity threat based on research of threat and plan of response to this threat.

The red team portion of the exercise seeks to identify the motivations, intent, tactics, targets, techniques, methods of operation, and capabilities of assigned cybersecurity threats (e.g., advanced persistent threats or APTs, hackers, etc.). The red team behaves like a threat actor (e.g., an APT or hacker) and creates a hypothetical cybersecurity incident based on what is known about the threat actor and the threat actor's capabilities. The blue team creates a cybersecurity strategy based on the information presented by the red team. The blue team examines measures that have been used to deal with the threat actor in the past, identifies flaws and gaps in these measures, identifies how it will respond to the cybersecurity incident identified by the red team, and recommends appropriate cybersecurity measures. A modified version of a red team/blue team exercise can be used in the field of cybersecurity as a tool to think about the entire cybersecurity preparedness cycle to deal with cybersecurity threats.

Creating a Preparedness Exercise

The first step in creating a preparedness exercise is to assess the current needs and capabilities of the agency with respect to incident response. The next step involves reviewing the incident response and or crisis management plans and identifying and reviewing the roles and responsibilities of individuals responsible for incident response. The next step is the identification of potential scenarios for cybersecurity incidents. These scenarios are used as the basis for the exercises that are developed. When drafting the exercise and the instructions for the exercise, it is important to include what the objectives of the exercise are and the metrics used to assess the performance of participants. The exercise should also include a segment which will enable participants to receive feedback on their performance and to identify any areas of improvement that are needed for the plan. The latter can include discussion that is held at the end of the exercise in a way to solicit feedback from participants and identify possible areas for improvement of the plan. This feedback and evaluation of the exercise can be provided within an evaluation form at the end of the exercise at the conclusion of the exercise. Following the completion of the exercise and after-action report is completed that documents the incident, actions of participants, and provides suggestions for plan improvement. This after-action report should be distributed to management and supervisors as well as other relevant stakeholders. Lessons learned should be communicated to these participants as well as to all employees within an organization who have some role in incident response. Any policy, procedure, and/or cybersecurity measure that has been identified as needed to deal with the cybersecurity threat of the scenario should also be implemented. Plan-based exercises are essential – they generate muscle memory for cybersecurity incident response, and they make the process and decision-making that occurs during cybersecurity incidents second nature to relevant stakeholders under conditions of stress.

Conclusion

Evaluating past responses to cybersecurity incidents and their impact on agencies and US national security interests provides practitioners with better insight as to how to handle such situations more effectively in the future. New threats emerge and existing threats evolve. Cybercriminals learn how to adapt to cybersecurity

measures; for this reason, it is important to consider cybersecurity as a continuous process that should adapt to changes in technologies and criminals' methods of operation.

Cross-References

- ▶ Cybersecurity: Incident Response
- ▶ Cybersecurity: Policy
- ▶ Cybersecurity: Practice

References

Brangetto, P., Çalişkan, E., & Rõigas, H. (2015). *Cyber Red Teaming: Organisational, technical and legal implications in a military context*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Cyber_Red_Team.pdf

CISA. (2019a). Cyber Storm: Securing cyber space. https://www.cisa.gov/cyber-storm-securing-cyber-space

CISA. (2019b). National Cyber Exercise and Planning Program. https://www.cisa.gov/national-cyber-exercise-and-planning-program

Dewar, R. S. (2018). *Cybersecurity and cyberdefense exercises*. Center for Security Studies (CSS) Cyber Defense Report, ETH Zürich. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf

DHS. (2012). Plan and prepare for disasters. https://www.dhs.gov/plan-and-prepare-disasters

DHS Ready. (n.d.). Exercises. https://www.ready.gov/business/testing/exercises

Emergency Management Institute (EMI). (n.d.). Discussion-based exercises. Federal Emergency Management Agency (FEMA). http://humtech.com/fema/isdbscourses/is703_nimsresource/RES0103350text.htm

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities. Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, 800–84. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

NYS-OEM. (n.d.). Exercises. http://www.dhses.ny.gov/oem/exercise/

Wilson, C. (2003). *Computer attack and cyber terrorism: Vulnerabilities and policy issues for congress*. CRS Report for Congress, RL32114. https://fas.org/irp/crs/RL32114.pdf

Further Reading

Brangetto, P., Çalişkan, E., & Rõigas, H. (2015). *Cyber Red Teaming: Organisational, technical and legal implications in a military context*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Cyber_Red_Team.pdf

Dewar, R. S. (2018). *Cybersecurity and cyberdefense exercises*. Center for Security Studies (CSS) Cyber Defense Report, ETH Zürich. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-10-Cyber_Exercises.pdf

D

Data Protection

M. Nazrul Islam
Farmingdale State College,
State University of New York,
Farmingdale, NY, USA

Keywords
Data breach · Data security · Data availability · Data management · Top secret data

Definition

Information: Anything that contains something which is timely delivered and will be useful to an audience.

Data: Binary bits stored on a digital media and processed by a processor. The bits can represent different types of information, text, audio, image, video, depending upon the software tool used to process the data.

Data security: Protection of digital data from unauthorized access, unintended modification, or fabrication, and ensuring safe delivery to authorized recipients.

Data breach: Unauthorized access to data.

Hardware: Digital devices that process, transmit, and store binary data.

Software: Programming codes that process binary data.

Introduction

We are living in a digital society where all our personal, social and professional activities involve either generation, processing, or storage of digital data. Every organization, small or large, private or federal, technical or nontechnical, deals with a huge amount of digital data, which contains either confidential, proprietary, or legal information; some may even be state top-secret information crucial to national security. With the growth of Internet, digital and communication technologies, and mobile applications, use of data is increasing at an exponential rate (Gartner 2018). This growth, in turn, raises the serious concerns of data security (Stalling and Brown 2018; Whitman and Mattord 2016). Protection of data from malicious attacks has become a great challenge for research and development (Muhleisen 2018).

The objective of this chapter is to present some fundamental concepts on the data security and protection techniques. It will begin with the basic characteristics of data from security perspectives. Threats to data will be discussed. Then different approaches to protect the data, including technological and sociological, will be presented.

Data Basics

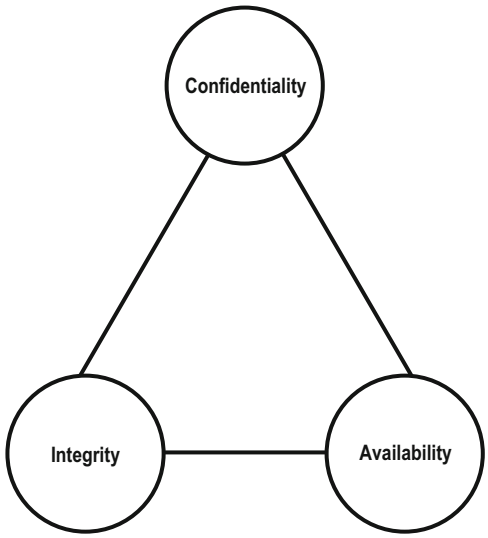
From digital point of view, data is simply a series of binary 1's and 0's stored in some electronic,

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

optical, or magnetic medium or transported through a network connection. Different groups of digital data represent different types of information, which could be text, graphics, audio, or video type. It is the set of hardware and software that translates between specific information and digital data. Therefore, security of data is primarily based on the type and importance of information.

"Information" is characterized by both "knowledge" and "communication" (Muhleisen 2018). Knowledge is recorded in some form, i.e., text, graphics, audio, video, and then is conveyed to its authorized user. Therefore, information is analyzed in security field by three main characteristics, namely, confidentiality, integrity, and availability (CIA). The first two characteristics connect to "knowledge," while the third one refers to "communication" of information. Information characteristics are often explained using a CIA triad as shown in Fig. 1 (Stallings and Brown 2018).

1. **Confidentiality**: Data is disclosed to only its authorized users. Any exposure to an unauthorized entity destroys the confidentiality of information, which may cause severe damage to the entities involved to the data.



Data Protection, Fig. 1 CIA triad of information security (Stallings and Brown 2018)

2. **Integrity**: Data remains whole, complete, and uncorrupted. Any malicious attack or simple technical failure may impact the consistency and accuracy of data which destroys its trustworthiness.
3. **Availability**: Data is available to its authorized user when asked for. Any interference or jamming in the communication medium or technical failure may cause unavailability of data which destroys the purpose of the information.

In addition to the above three prime characteristics, data is also described by a number of other parameters, some of which are listed below.

1. **Accuracy**: The data delivered to the end user must contain the correct information. If the information is false or manipulated, the data loses its accuracy.
2. **Authenticity**: The data communication includes the information about the source/sender. It must be received from the right source as it pretends to be.
3. **Utility**: The data must have some value or meaningful purpose to the end user when received.
4. **Possession**: The source/sender and the destination/receiver must have appropriate legal rights concerning the data.

Data is also characterized by its state, which includes:

1. **Storage**: Data is saved in a medium, which determines the accuracy and integrity of data.
2. **Processing**: Data is processed using hardware and/or software, which determines the utility of data.
3. **Transmission**: Data is traversing a network, which determines authenticity, integrity and availability of data.

Data Security

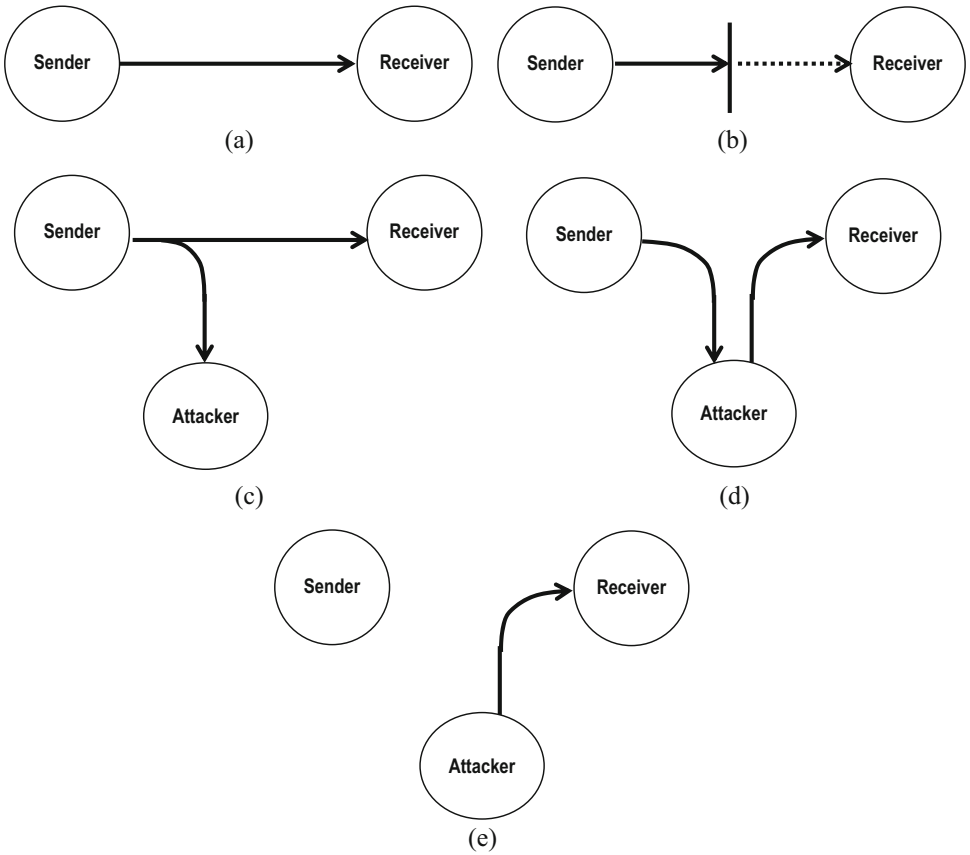
Before we talk about data protection, we need to understand how data can be hacked and hence loses its characteristics. As data is processed,

stored, and transmitted using widely available digital technologies, it is vulnerable to a variety of threats. As a result, security of data and hence information is very crucial to individual, organizational, and even national interests. Typical motives for malicious attacks on data include the following (Whitman and Mattord 2016).

1. Status: Some people, who are computer savvy, play with software tools to destroy or manipulate some data just for fun.
2. Revenge: People may take revenge by misusing some confidential data. For example, a terminated employee may destroy the company data.
3. Economic gain: People or competing organizations may attack secure data for financial purposes.
4. Political achievement: Use of cyber domain is increasing for political movement, propaganda, spying and even civil war.

There are many different ways that confidential data can be attacked. Most of the attacks are involved to the communication network as shown in Fig. 2a. The attack techniques can be categorized into the following four main groups (Fadia and Zacharia 2008).

1. Interruption: The communication between the sender and the receiver is interrupted or the source system is attacked such that the receiver cannot get the requested service from it as depicted in Fig. 2b. The availability characteristics of data are lost.



Data Protection, Fig. 2 Attack technologies: (**a**) ideal communication network, (**b**) interruption, (**c**) interception, (**d**) modification, (**e**) fabrication

2. Interception: Figure 2c demonstrates how an unauthorized party intercepts the communication silently without the knowledge of sender or receiver and gets access to data. Data is no longer confidential.
3. Modification: The attacker interrupts the direct communication between sender and receiver and diverts the data to itself as shown in Fig. 2d. Then it sends the modified data to the receiver. The integrity of data is lost.
4. Fabrication: The attacker sends false data to the receiver pretending itself as a legitimate sender as demonstrated in Fig. 2e. The authentication of data fails.

Data Protection

Data protection is a complex process because it involves multiple different entities. In general, a data system includes the following components (Stair and Reynolds 2017):

1. Hardware
2. Software
3. Data
4. Network
5. People
6. Procedure

Threats to data can occur from any of the above components. As a result, a comprehensive data protection strategy needs to include the following three approaches:

1. Technology
2. Policy
3. Education

In each of these categories, there is no single solution, rather a combination of multiple strategies.

Technological Solutions to Data Protection

Technological solutions depend on the status of data, whether in storage, or processing or in transmission. There are three main principles of data protection techniques:

1. Preventing access to data
2. Making data unreadable
3. Monitoring data

Preventing Access to Data

The best approach is to make the confidential data completely inaccessible by any unauthorized party. Several techniques can be incorporated which will control and even block the communication to the data to be protected.

Firewall: A hardware technique or a software tool or a process or a combination to control and monitor the access requests to any data. Usually placed in the perimeter of a network, it checks for any malicious code or suspicious network communication to and from the data source.

Proxy Server: Conceals the secure data source in a network by isolating from the external network. Ensures the anonymity of internal hosts and acts on its behalf to receive, process, and respond to any data communication requests from outside network.

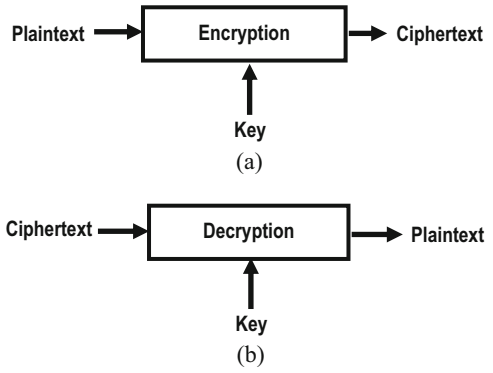
Bastion Host: System designed to represent the internal network to the outside world and withstand any attack targeted to secure data or systems.

Device Authentication: Any device plugged into a system or network needs to be authenticated before accessing or processing data.

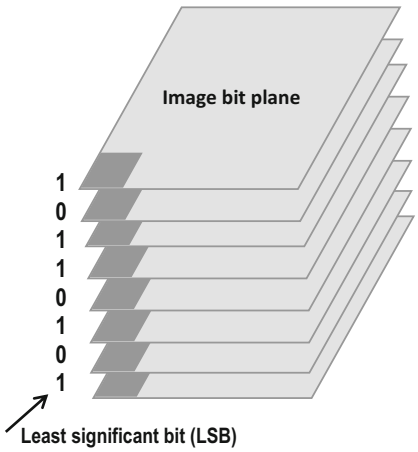
Making Data Unreadable

Data is scrambled or hidden so that an intruder cannot read or interpret the data even if he/she gains access to it. There are two main data scrambling techniques:

Cryptography: Convert the data to a different form such that it is either unreadable or unusable by any intruder. A mathematical or logical algorithm translates the plaintext data using a single or a set of secret keys to a ciphertext data as demonstrated in Fig. 3. Only an authorized user having the right key can decrypt the ciphertext data back to plaintext data and then use it. Cryptographic techniques vary in encryption/decryption algorithms and selection and management of secret keys.



Data Protection, Fig. 3 Cryptography principle: (**a**) encryption, (**b**) decryption



Data Protection, Fig. 4 Steganography principle

Steganography: Process of hiding data inside other data which can be open to public. The most popular technique is hiding the data inside an image. The image before hiding data is called a cover image and that with data hidden is called a stego image. As shown in Fig. 4, the least significant bits of pixels are replaced by the confidential data such that the overall intensity or color of the stego image will not be significantly different from the cover image. There are more complex algorithms for choosing bits from the cover image and replacing them with data bits (Islam et al. 2015). Similarly, the confidential data can be hidden in a text message between alphabets by altering the given bits.

Monitoring Data

A hardware or software or a combination tool can be designed to constantly monitor all of the activities with data in all three phases of data, storage, processing, and transmission. It logs each activity, distinguishes between authorized and suspicious activities, and generates alert messages for the data owner, user, or manager. In a network, it performs intrusion detection live. A smarter tool can also be designed to stop the suspicious activity as soon as it is detected.

Law and Policy for Data Protection

As data involves human users, in addition to hardware and software, only technological solutions cannot ensure data protection. Therefore, data protection approaches involve laws and policies.

Data Protection Act

European Union's General Data Protection Regulation (GDPR) was transposed into the United Kingdom's law as the "Data Protection Act 2018" to control personal information used by any organization. It ensures the proper use of data.

1. Data is used fairly, lawfully and transparently.
2. Data is used for specified and explicit purposes.
3. Data is used in a way that is adequate, relevant and limited to only what is necessary.
4. Data is accurate and, where necessary, kept up to date.
5. Data is kept for no longer than is necessary.
6. Data is handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage.

The Act gives an individual the following rights on a personal data stored by an organization.

1. Know how the data is used.
2. Access the data.
3. Update any incorrect data.
4. Erase data.
5. Stop or restrict processing the data.

6. Receive and reuse data for different services.
7. Monitor how data is processed in certain circumstance.

Security Policy

A data protection policy is usually designed by an organization to govern the data usage and prosecution procedure. A typical policy typically includes the following components:

1. How to use the organization's data resources safely.
2. How to respond to any data breaches.
3. What defenses should be incorporated.

There are certain guidelines on how to devise an effective data protection policy (Whitman and Mattord 2016):

1. It needs be comprehensive and include all possible scenarios.
2. It should be open to revisions and updates.
3. It should be simple and easy to understand.
4. It should define what data and activities are subject to organization policy.
5. It should be available to all data users.
6. There should be a procedure to enforce the policy while data is in use.
7. Users should be warned about the penalty for mishandling data.

Security Awareness

No matter how sophisticated technology is implemented and/or how vibrant policy is devised, data will not be safe unless the human users are well educated and well aware of consequences of data breaches. The users must understand the significance of data to the organization, learn the technology and how to use data, and realize the penalty for policy violation.

Security awareness can be incorporated through a number of activities as follows.

1. Security Training: The users need be trained on the data usage and protection schemes. Such training must be included in the new-employee orientation program. In addition, there should be frequent workshops and seminars to keep them updated on the data protection technique and policy.
2. Security Drills: Like fire drills, security drills can be designed and implemented in order to assess the users' performance in case of malicious incidences.
3. Security Alerts: Warning messages, emails, pop-up windows, and several other strategies should be adopted to keep the users aware of data protection techniques and policies.

Conclusion

Digital data contains confidential information that are crucial to individuals, organizations and the nation. Data needs be protected from access, modification or destruction by any unauthorized party. There are three approaches to protect data, namely, technology, policy, and education. Technological schemes involve hardware and software tools to prevent access to data, hide data from intruder, and constantly monitor the data operations. Laws and policies reserve the rights of different entities involved to data, namely, users, owners, senders, and recipients. Finally, security awareness programs, including training, drills, and alerts, educate the users and keep them updated on the safe usage of data.

The world is moving around digital data which are very vulnerable to many different types of attacks. The most challenging part is that the hackers are always developing new attack technologies. Therefore, data protection techniques should be innovative, dynamic, and proactive. All three approaches to data protection, technology, policy, and education need to function efficiently, in synchronization and in depth in order to defend against any malicious attack on data.

References

Data Protection Act. (2018). http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Fadia, A., & Zacharia, M. (2008). *Network intrusion alert: An ethical hacking guide to intrusion detection*. Boston, Massachusetts: Course Technology.

Gartner. (2018). Gartner worldwide IT spending forecast, *Gartner Market Databook*. https://www.gartner.com

Islam, M. N., Islam, M. F., & Shahrabi, K. (2015). Robust information security system using steganography, orthogonal code and joint transform correlation. *International Journal for Light and Electron Optics, 126*, 4026–4031.

Muhleisen, M. (2018). The long and short of digital revolution. *Finance & Development*, International Monetary Fund.

Stair, R. M., & Reynolds, G. W. (2017). *Fundamentals of information systems*. Boston, Massachusetts: Cengage Learning.

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Upper Saddle River, New Jersey: Pearson.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security*. Boston, Massachusetts: Cengage Learning.

Further Reading

Bala, D. (2008). Biometrics and information security. Proceedings of the 5th annual conference on Information security curriculum development (InfoSecCD '08) ACM, 64–66.

Chen, D., & Zhao, H. (2012). *Data security and privacy protection issues in cloud computing*. IEEE International Conference on Computer Science and Electronics Engineering.

Hayden, L. (2010). IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data.

Islam, M. N. (2011). Encryption and multiplexing of fingerprints for enhanced security. Proceedings of IEEE Long Island Systems, Applications and Technology Conference (LISAT).

Kaufman LM (2009). Data security in the world cloud of computing. *IEEE Security and Privacy, 7*(4): 61–64.

Krutz RL & Vines RD (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing.

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. 17(1): 51–58.

Department of Homeland Security (DHS)

Jennifer Bencivenga
John Jay College of Criminal Justice, City University of New York, New York, NY, USA

D

Keywords

Department of Homeland Security (DHS) · Domestic terrorism · International terrorism · 9/11 · Public security · Private security · Public-private partnership · Hometown security · Fusion center · Intelligence · Soft target · DHS operational and support components · Homeland Security Act · Presidential Policy Directive 2

Definition

Department of Homeland Security: a federal agency, created in the wake of the terrorist attacks of 9/11, tasked with leading the national effort to protect the United States from terrorism

Introduction

The Department of Homeland Security (DHS) is a federal agency originally created to counter the threats of terrorism but has expanded its responsibilities to combat crime and provide expeditious response and support during emergencies. Currently, the DHS core duties include preventing terrorism and enhancing security, securing and managing borders, enforcing and administering immigration laws, safeguarding and securing cyberspace, ensuring resilience to disasters, and maturing and strengthening the homeland security enterprise.

The current mission of the DHS is "With honor and integrity, we will safeguard the American people, our homeland, and our values" (DHS

2016). However, the DHS cannot effectively protect the homeland alone. Evolving threats, expansive skillsets of malicious actors, and vulnerabilities to critical infrastructure create a difficult and complex operation for the DHS. Through its cooperation with the federal government and state, local, tribal, and territorial (SLTT) partners, as well as its relationship with the private sector, the DHS is better equipped to meet growing security needs.

Over the past 16 years, the DHS has faced several challenges and criticisms. From its massive size to its multibillion dollar budget requests, skeptics consistently call into question the DHS's capabilities and successes. Dynamics within the DHS's operational constructs and external political factors have impacted the many ways Americans view the organization and the future of homeland security.

History

Though the origins of homeland security are often associated with the devastating attacks on 9/11, domestic terrorism has been a concern for the United States government and the American people since the nineteenth century (e.g., the Black Panthers, the Ku Klux Klan, the Workers Party, the communist agitators, the Students for a Democratic Society, the Weathermen of the Vietnam Era). According to Nemeth (2017), "the concept of terror against governing authority was entrenched into the political and social fabric of these organizations" (p. 15). The United States had also experienced international terrorism pre-9/11, at home and abroad (Nemeth 2017). Though terrorism was not a new term during the pre-9/11 era, the concept of homeland security was not as widely understood.

Prior to 9/11, Islamist extremists had provided "plenty of warning that they meant to kill Americans indiscriminately and in large numbers" (9/11 Commission Report, 2004, para. 9). On home soil, the 1993 WTC bombing that killed six was led by Ramzi Yousef, who also planned to blow up United States airliners over the Pacific in 1995 (9/11 Commission Report, 2004). Overseas, there was the 1983 terrorist attack against the United States Marine base in Beirut, Lebanon, which killed 241 servicemen (Nemeth 2017). In 1998, there were several truck bombings at US embassies, carried out by al-Qaeda, in Nairobi, Kenya, and Tanzania (9/11 Commission Report, 2004). Though not as sophisticated as the coordinated attacks on 9/11, these terrorist attacks, among several others, should have indicated to law enforcement and the intelligence community that Osama bin Laden's al-Qaeda would continue to relentlessly target Americans.

In the weeks and months following the attacks on 9/11, it became apparent that there were operational, intelligence, aviation security, and border and immigration control issues (9/11 Commission Report, 2004). In reviewing and evaluating such failures, the Bush administration made it a priority to never let another attack like 9/11 happen again. In November 2002, the Homeland Security Act was stood up to create the DHS. This Act, which created offices and directorates within the DHS, reflected the concept that terrorism prevention was now at the forefront of security. As years passed, additional DHS laws concerning emergency management, immigration and border security, maritime security, and transportation security were also passed.

Organization

Since its inception, the DHS operational and support components were brought together to serve as one unified front. Currently, there are 14 agencies operating under DHS supervision (see Table 1). As expected, the Office of the Secretary has changed and developed since its early beginnings, housing several other offices, including the Office of Public Affairs, Privacy Office, and Partnership and Engagement. On December 6, 2017, Kirstjen Nielsen was sworn in under President Trump as the sixth Secretary of Homeland Security and has focused on the immigration laws and policies that have been at the center of President Trump's administration. However, this is not to say that Secretary Nielsen's attention has not been focusing on other issues, for example, election

Department of Homeland Security (DHS), Table 1 Agencies under DHS supervision

Countering Weapons of Mass Destruction Office	Cybersecurity and Infrastructure Security Agency	Federal Emergency Management Agency	Federal Law Enforcement Training Center
Office of Intelligence and Analysis	Office of Operations Coordination	Management Directorate, Science and Technology Directorate	Science and Technology Directorate
Transportation Security Administration	United States Citizenship and Immigration Services	United States Coast Guard	United States Customs and Border Protection
United States Immigration and Customs Enforcement	United States Secret Service		

interference. Secretary Nielsen recently said, "Election security wasn't a mission we envisioned for the department when it was created, but it's now one of my highest priorities" (Tuttle 2018, p.20). These examples demonstrate that DHS handles much more than what typically is believed to be in its purview.

Another construct within DHS is its several advisory panels and committees, which provide guidance on mission-related topics. Mission-related topics include academic engagement, counterterrorism committees and working groups, and immigration committees and working groups, among others. Of great prestige is the Homeland Security Academic Advisory Council, which "provides advice and recommendations to the Secretary and senior leadership on matters related to homeland security and the academic community, including: student and recent graduate recruitment; international students; academic research and faculty exchanges; campus resilience; homeland security academic programs; and cybersecurity" (DHS 2018a, para. 1). These advisory panels and committees are just a small sampling of the programs DHS has in place for engaging with Americans and the private sector.

Public-Private Partnership

The DHS has established several programs and campaigns to bring awareness to critical infrastructure owners and operators, as 85% of critical infrastructure ownership belongs to the private sector (U.S. GAO 2006). This high percentage of ownership is attributed to:

> 1.) the perception that the private sector is better placed to efficiently manage different sectors of activity, including security ones, thanks to its organizational structure and existing expertise; and
> 2.) the enlargement of the concept of critical infrastructure, which evolved from being equated with military structures to being associated with more diverse forms of infrastructure such as economic ones. (Bures and Carrapico 2017, p. 232)

As such, since majority of stakeholders represent the private sector, public-private collaboration is a necessity.

The homeland security enterprise benefits from public-private partnerships, as they can enhance hiring, resource utilization, specialization, cross sector trust, and technological innovation (Busch and Givens 2012). Additionally, partnerships aid in intelligence sharing, which can lead to swift response during emergencies and terrorist attacks. These partnerships go beyond contractual agreements and government-business relationships and instead represent a more dynamic and meaningful collaboration to contribute to homeland security than any one agency could alone.

The Presidential Policy Directive 21: Critical Infrastructure Security and Resilience recognizes 16 critical infrastructure sectors (see Table 2). Though each sector serves the interests of the American people in a different capacity, interdependencies exist across sectors. The holistic vitality of the entire critical infrastructure system is interconnected, and if one sector were to be incapacitated, the entire system would be left vulnerable.

Department of Homeland Security (DHS), Table 2 16 Critical infrastructure sectors

Chemical	Commercial facilities	Communications	Critical manufacturing
Dams	Defense industrial base	Emergency services	Energy
Financial services	Food and agriculture	Government facilities	Healthcare and public health
Information technology	Nuclear reactors, materials, and waste	Transportation	Water and wastewater systems

Several public-private programs have been established to bring awareness to critical infrastructure homeland security issues and to problem solve difficult issues pertaining to critical infrastructure vulnerabilities and threat exploitation. For example, the DHS Science and Technology Directorate Silicon Valley Innovation Program was established to find "new technologies that strengthen national security with the goal of reshaping how government, entrepreneurs, and industry work together to find cutting-edge solutions" (DHS, n.d. para. 1). Other programs, such as the SAFETY Act, which support the development and deployment of anti-terrorism technologies, provide incentives to partners. These programs aid in the flow of intelligence sharing between the public and private sector.

A major facilitator of intelligence sharing is through the National Framework of Fusion Centers. A fusion center is a state and major urban area focal point for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government, SLTT, and private sector partners (DHS 2018c). A fusion center may seat representatives from a variety of law enforcement and emergency services disciplines, and, in theory, this "diverse composition of organizations is best positioned to identify and understand threats facing a particular jurisdiction or region" (Carter et al. 2017, p. 11–12). The fusion center engages local and regional partners on all threats and all hazards, serving as the one-stop shop for homeland security and crime requests and inquiries.

The Boston Regional Intelligence Center (BRIC), an urban area fusion center in Massachusetts, works with the private sector through the BRIC Shield. The BRIC Shield is a membership program that provides customers with threat information and situational awareness (BRIC 2018). Through this membership, private sector partners stay abreast on pertinent homeland security and crime issues. Other intelligence sharing programs within the BRIC and fusion centers across the country exist, including the Homeland Security Information Network, which is the trusted portal for sharing unclassified information (HSIN, 2018).

Hometown Security

In recent years, safety and security for soft targets and crowded places have become a focus for policy makers and public safety professionals. Places that are publicly accessible, where people gather freely, such as concerts, sporting events, subways, or malls, and have minimal security are vulnerable to attack (DHS 2018d). These types of areas have been intensely targeted in the past as they provide unsophisticated means for a malicious actor to carry out an attack. Attacks may include improvised explosive devices, vehicle ramming, or mass shootings.

Unfortunately, active shooter incidents in populated areas have drastically increased in recent years. In 2016 and 2017, there were 50 incidents in 21 states resulting in 943 casualties, 712 casualties from 2014 and 2015, which experienced 20 incidents in 26 states resulting in 231 casualties (FBI, 2018). And, within the first 45 days of 2018, there were 17 school shootings (Galea et al. 2018). On February 14, 2018, the Marjory Stoneman Douglas High School shooting, which resulted 17 causalities, led to "unprecedented action, including some of the largest and most prominent gun dealers and retailers, such as Dick's Sporting Goods and Walmart, [to] voluntarily [stop] the

sales of assault weapons and [increase] the age at which customers can buy certain firearms" (Galea et al. 2018, p. 858). Such horrific acts of violence have led not only private sector companies to forge change but also the DHS through its hometown security programs.

One of the more popular programs is the "If You See Something, Say Something" campaign. This program encourages citizens to stay alert and report suspicious activity to local law enforcement to protect the community (DHS, n.d.). The DHS has designated September 25 as National Awareness Day, indicating that "informed, alert communities play a critical role in keeping our nation safe" (DHS, n.d., para. 2). Aside from this campaign, DHS also provides the community with free and accessible resource guides and threat assessment models. The people living and working in any community are the eyes and ears for law enforcement.

Perception of DHS

As with all major legislative laws and policies, especially those related to the DHS, researchers, academics, and practitioners undoubtedly point out flaws and challenges within the Department. When the 2002 Office of Homeland Security's National Strategy for Homeland Security was introduced, it came under scrutiny for various reasons including its "fuzziness of roles and responsibilities across existing and planned homeland security programs" (Caudle 2003, p. 22). Given the sheer size of the DHS, which today requires the employment of over 240,000 workers, it is not farfetched to believe that transparency and efficiency are overshadowed by bureaucracy and misplaced power.

Even after the first 10 years of operation, it was still believed by some critics that DHS and its Science and Technology Directorate were underperforming. Again, pointing to the "heterogeneous and immiscible collection of agencies with different cultures, policies, traditions, missions, and responsibilities," it was ascertained that a unified effort was merely inconceivable (Zimmerman 2011, p. 153). The issue was not that intentions were misplaced but instead that the strategies that were implemented were completely misguided and illogical. One of the major concerns with the Science and Technology Directorate was its budget. From the start, the Science and Technology Directorate was criticized for "funneling funding exclusively into the Department of Energy national laboratories, rather than supporting university-based programmes or private-sector research" (Zimmerman 2011, p. 154). It is believed that the allocation to these labs "may have precluded the innovations that might have come from a more broadly sourced effort" (Zimmerman 2011, p. 154).

The concern for misplacement of power and funding has been covered recently in mainstream news media, especially when considering the detention of immigrant children. It is believed the DHS facilities do not meet the "basic standards for the care of children in residential settings" and that there should be "limited exposure of any child to current DHS facilities (i.e., Customs and Border Protection and Immigration and Customs Enforcement facilities)" (Linton et al. 2017, p. 1). It has been reported that many detention centers lacked bedding and bathing facilities, did not provide sufficient food or water, and kept children and families in extremely cold temperatures (Linton et al. 2017, p. 4). These conditions, coupled with the separation of children from their biological parents or legal guardians (when unable to prove relation), have traumatized detained children.

Conclusion

The DHS is a young federal agency tasked with a major responsibility – keeping America safe. Since 9/11, the prevention of terrorism has been at the forefront of security professionals' minds. From major event protection to school safety, from aviation security and cybersecurity, the DHS has its hands in all mission-related operations. Though the future of homeland security is unclear, the fact remains that as long as terrorism exists, so too does the need for enhanced security, forward thinking, and meaningful decisionmaking. For the DHS to thrive in the

coming years, it cannot "use law enforcement techniques suitable for the twentieth century" (Nemeth 2017, p. 531). Instead technology needs to be researched and put to efficient and reasonable use as it pertains to preventing terrorism and crime and responding to natural disasters.

Cross-References

- ▶ Border Security
- ▶ Critical Infrastructure Protection
- ▶ Homeland Security Act of 2002
- ▶ Emergency Management: International
- ▶ Event Security
- ▶ Federal Emergency Management Agency
- ▶ Intelligence
- ▶ Public-Private Partnerships: Port Security

References

Boston Regional Intelligence Center. (2018). *BRIC Shield.* Retrieved from: https://bostonbric.org/default.aspx?menuitemid=10684

Bures, O., & Carrapico, H. (2017). Private security beyond private military and security companies: Exploring diversity within private-public collaborations and its consequences for security governance. *Crime, Law and Social Change, 67*(3), 229–243.

Busch, N., & Givens, A. (2012). Public-private partnerships in homeland security: Opportunities and challenges. *Homeland Security Affairs, 8*(1), 1–24.

Carter, J., Carter, D., Chermak, S., & McGarrell, E. (2017). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. *Journal of Police and Criminal Psychology, 32*(1), 11–27.

Caudle, S. (2003). Homeland security: A challenging environment; The meaning of homeland security, its intent, and the key issues officials will encounter in addressing its policy and management challenges. *The Public Manager, 32*(1), 19.

Department of Homeland Security. (2016). *Mission.* Retrieved from: https://www.dhs.gov/mission

Department of Homeland Security. (2018a). *Homeland security academic advisory council.* Retrieved from: https://www.dhs.gov/homeland-security-academic-advisory-council-hsaac

Department of Homeland Security. (2018c). *National network of fusion centers face sheet.* Retrieved from: https://www.dhs.gov/national-network-fusion-centers-fact-sheet

Department of Homeland Security. (2018d). *Securing soft targets and crowded spaces*. Retrieved from: https://www.dhs.gov/securing-soft-targets-and-crowded-spaces

Department of Homeland Security. (n.d.-b). *See something, say something.* Retrieved from: https://www.dhs.gov/see-something-say-something

Department of Homeland Security. (n.d.-c). *See something say something awareness day.* https://www.dhs.gov/see-something-say-something/about-campaign/seesay-day?utm_source=seesay_slideshow&utm_medium=web&utm_campaign=dhsgov

FBI Active Shooter Incidents in the United States 2018 https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2018-041019.pdf/view

Galea, S., Branas, C. C., Flescher, A., Formica, M. K., Hennig, N., Liller, K. D., et al. (2018). Priorities in recovering from a lost generation of firearms research. *American Journal of Public Health, 108*(7), 858–860.

Homeland Security Information Network 2018 Annual Report https://www.dhs.gov/sites/default/files/publications/hsin-fy2018-annual-report.pdf

Linton, J., Griffin, M., & Shapiro, A. (2017). Detention of immigrant children. *Pediatrics, 139*(5), E20170483-0483v1.

Nemeth, C. (2017). *Homeland security: An introduction to principles and practice* (3rd ed.), CRC Press, Taylor and Francis.

Tuttle, H. (2018). Hack the vote2. *Risk Management, 65*(9), 20–22, 24–25.

U.S. Government Accountability Office. (2006). *Critical infrastructure protection: Progress coordinating government and private sector efforts varies by sectors' characteristics.* Retrieved from: https://www.gao.gov/products/GAO-07-39

Zimmerman, P. D. (2011). Homeland insecurity: In ten years of operation, the unwieldy Department of Homeland Security and its science directorate have seriously underperformed. *Nature, 477*(7363), 153.

Further Reading

Department of Homeland Security. (2018b). *Homeland Security Information Network (HSIN)*. Retrieved from: https://www.dhs.gov/homeland-security-information-network-hsin

Department of Homeland Security. (n.d.-a). *Science and technology silicon valley innovation program.* Retrieved from: https://www.dhs.gov/science-and-technology/svip

National Commission on Terrorist Attacks Upon the United States. (2004). *Final report of the National Commission on Terrorist Attacks Upon the United States.* Retrieved from: https://govinfo.library.unt.edu/911/report/911Report_Exec.htm

The White House Office of the Press Secretary. (2013) *Presidential policy directive 21: Critical infrastructure security and resilience.* Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks Upton the United States authored by the 9/11 Commission.
Intelligence. From Secrets to Policy, seventh Edition authored by Mark M. Lowenthal.
Homeland Security. An Introduction to Principles and Practices, third Edition authored by Charles P. Nemeth.
U.S. Department of Justice Federal Bureau of Investigation. (2018). *Active shooter incidents in the United States in 2016 and 2017*. Retrieved from: https://www.fbi.gov/file-repository/active-shooter-incidents-us-2016-2017.pdf/view

Drones

E. Parrott
Liverpool John Moores University,
Liverpool, UK

Keywords
Drone · Unmanned aerial vehicle · Unmanned aircraft system · Remote sensing · Surveillance · Privacy · Reconstruction

Definition

A drone, otherwise referred to as an unmanned aerial vehicle (UAV) or unmanned aircraft system (UAS), is a remotely piloted aircraft that is typically controlled via a handheld transmitter, computer-based ground station, or an onboard computer, when operating autonomously.

Introduction

Unmanned aircraft systems (UASs) or unmanned aerial vehicles (UAVs), otherwise known as drones, are becoming increasingly commonplace among law enforcement worldwide. As UAV devices are providing operators with real-time situational awareness while replacing personnel in tasks considered to be too dull, dirty and dangerous (Marshall 2004). Previously, drone technology only encompassed large military systems deployed overseas for reconnaissance and combat use. However, over the last decade, the emergence of sophisticated micro aerial vehicles (MAVs) and smaller UAVs (<20 kg) has led to the use of UAV technology across every sector. As a result of this, UAV technology is also increasingly used internationally among emergency first responders and law enforcement as a low-cost tool for tackling crime and responding to mass incidents. This is because UAV technology has the ability to provide operators with real-time situational awareness, by assessing large and potentially hazardous environments from new perspectives, using a range of data capture methods, without having to factor in high staffing costs or risk to personnel.

Although increasing use of UAV technology has predominantly been positive, criminal and terror groups have also found ways to profit from the utilization of drone technology, with increasing incidents occurring worldwide. Consequently, illegal use of drone technology is a prevalent issue facing law enforcement agencies and governments. However, citizens and businesses are also using drones for recreational and security purposes. As such, crucial decisions are currently being made regarding how to police, search, and seize criminal UAV devices, as well as to manage the illegal activity by criminals. Lawmakers and enforcers are also attempting to determine the best way to preserve a safe airspace for noncriminal users while ensuring the safety and privacy of the public in general.

This entry provides an overview of UAV technology used by emergency and security management personnel for crime prevention and emergency assistance. Specifically, an explanation of UAV technology has been included to aid readers' understanding of these devices and their capabilities within different scenarios. Section "Drone Principles, Systems, and Payload" of this entry explores different drone technologies, summarizing their general characteristics and components. The aim is to inform practitioners about these devices, whether encountered as a tool within law enforcement or as an evidential item seized during investigation. Section "Criminal Drone Use and Threats to Security" summarizes how criminals use drones, with examples of

previous incidents that have caused security breaches or damage. Section "Drone Use in Law Enforcement" describes current law enforcement drone use, outlining the different applications of how police officers and other emergency first responders use this technology. Finally, Section "Drone Legislation and Public Perception" outlines general drone legislation for both members of the public and law enforcement.

Drone Principles, Systems, and Payloads

Within the last decade, the commercial drone industry has grown significantly as new devices are continually developed for emerging applications. Yet, in spite of the extensive range of shapes, sizes, payloads, and capabilities, generally, all UAV systems can be categorized as either fixed-wing or multirotor UAVs, with some exception (Wingtra 2019).

Fixed Wing

Fixed-wing UAVs most resemble traditional manned aircraft, as a fixed-wing drone typically includes a central body, single propeller, and two wings. Much alike manned aircraft, fixed-wing UAVs generate and maintain the aerodynamic force lift, as air flows over and beneath the surface of the wing or airfoil creating areas of low and high air pressure, respectively. As such, fixed-wing UAVs are controlled by the movement and positioning of the ailerons and rudder surfaces to control the roll, pitch, and yaw of the aircraft, though these control surfaces differ greatly among devices (Fahlstrom and Gleason 2012).

The main advantage of fixed-wing UAVs is their ability to achieve much greater flight times (i.e., over multiple hours), as fixed wings are able to cover much larger spaces with a lower power consumption in comparison with multirotors (Boon et al. 2017). However, similarly to manned aircraft, fixed-wing UAVs require space for landing and takeoff. Takeoff is generally achieved by throwing the aircraft or using a catapult-like system (Fahlstrom and Gleason 2012). Also, as fixed-wing UAVs rely upon airflow to maintain flight, they are unable to hover or yaw on the spot. Because of this limitation, fixed wings rely upon banking turns that require a large operating space, making them difficult to maneuver in confined spaces.

Multirotor

As multirotor UAVs make up the majority of the commercial market and consumer models, they are the most common type of drone used by commercial operators as well as hobbyists and researchers. In contrast to fixed-wing UAVs, multirotors generate and maintain stable flight through the rotation of paired counterrotating propellers. Although a multirotor is defined as anything with two or more rotors, generally, the most popular configurations are quadcopters (four propellers), hexacopters (six propellers), and octocopters (eight propellers) (Fahlstrom and Gleason 2012).

Unlike fixed-wing UAVs, multirotors can achieve vertical takeoff and landing (VTOL) and are able to hover and yaw on the spot. This type of maneuverability makes multirotors commonly favored in congested or confined spaces (Castillo et al. 2017), particularly for filming or surveillance applications (see chapter ▶ "Investigations: Accidents and Reconstructions"). However, in comparison with fixed-wing UAVs, multirotors are much more power intensive, with flight times typically lasting under an hour on one battery.

Components

Although the airframes and control surfaces of multirotors and fixed-wing UAVs differ significantly, many of the internal components are identical and merely configured to suit the airframe and purpose of the aircraft. As such, fixed-wing and multirotor UAVs generally both include flight controllers (FCs), electronic speed controllers (ESCs), and brushless direct current (BLDC) motors and propellers, as well as a lithium-polymer (Lipo) battery/batteries to power the aircraft and a receiver (Rx) usually paired to a handheld transmitter (Tx) for piloting and controlling the aircraft (Quan 2017). The FC acts as the central brain of the aircraft for movement, control, and feedback. FCs are essential for receiving user commands and converting them into control

movements, as well as providing feedback from the aircraft using integrated onboard sensors, including accelerometers, gyroscopes, barometers, and magnetometers.

Also connected to the FC, ESCs receive a control command and convert this into a three-phase alternating current (AC) power, to power the BLDC motor and therefore spin the connected propeller. Depending on the configuration of the drone, the number of ESCs, motors, and propellers will differ; for example, a quadcopter will have four ESCs, motors, and propellers. A fixed wing may only have one single ESC, motor, and propeller, allowing the ailerons and rudder to be controlled by additional servo motors mounted on the aircraft (Fahlstrom and Gleason 2012). In addition, the FC may be a central hub for additional peripheral sensors, including a global positioning system (GPS) unit, typically used for flight stability, positional control and as a pilot aid. Or a number of other sensors used for object collision avoidance (i.e., ultrasonic, infrared, or stereovision cameras) or as additional pilot aids, for example, laser emitting diode (LED) lights, buzzers, and speakers.

Operation

Much alike the extensive variety of UAV devices, the setup and operation of these systems is equally varied. Although these systems may be controlled with something as simple as an app on a phone, most professional UAVs use either a traditional handheld Tx, with access to a range of flight modes with varying levels of pilot assistance, or a computer-based ground station. This is generally more common when controlling fixed-wing UAVs as these systems are generally used to conduct waypoint flying (a semiautonomous flight mode where an aircraft is pre-programmed with a sequence of GPS locations (ArduPilot 2019b)). Some systems, such as research-based systems, are controlled via an onboard computer, but these UAVs are beyond the scope of this entry.

To further aid the pilot, most UAV systems (i.e., DJI and Pixhawk) will have a LED indicator present to inform the pilot of the current status of the UAV while it is powered. These LED indicators will commonly flash different colors at different rates to inform the pilot of the current flight mode selected, whether the system has established a GPS lock (of a number of satellites as predetermined depending on the configuration of the device) or whether fail-safe is enabled, as well as being an indicator for any other potential errors, for example, battery warning and compass calibration (ArduPilot 2019a). Hence, it is therefore essential that any UAV pilot be aware of the LED indicator sequence relevant to their device as these differ significantly among models and manufacturers.

However, in the event of an emergency, the majority of UAVs come with pre-programmed fail-safes which are configured by the user during setup. Fail-safes, sometimes otherwise referred to as return to home (RTH) or return to land (RTL), are generally engaged by either the pilot in the event of an emergency, by a spotter in the case of pilot incapacitation or by the hardware during a loss of signal (DJI 2019a). As such, commercial Tx controllers usually come with a pre-programmed RTL fail-safe switches (on custom systems fail-safe switches can be selected by the user on programmable controllers (FrSky 2019)). Depending on the setup and control methods of the UAV, once engaged fail-safe programs will either attempt to return the drone to its initial takeoff positon (as determined from GPS data) or slowly descend to land in the positon that the switch was engaged in the case of multirotors or attempt a controlled descent in the case of fixed wings.

Payloads

As the value of UAV technology has been recognized within many applications, specific UAV payloads are being continually developed to meet the increasing application demands. With regard to this, many sensors are now custom developed for UAV use. For all UAV technology, weight is a significant consideration for flight time and power consumption. As such, advanced manufacturing capabilities allow UAVs to carry all manner of electronic and optical devices previously only suited to large and expensive manned aircraft.

The complete range of payloads available for UAVs is extensive and beyond the scope of this entry. Therefore, only the most popular payloads commonly integrated or attached to commercial drones with relevance to emergency and security management have been included.

Digital Cameras. Typical red-green-blue (RGB) digital cameras are the most prevalent integrated or added UAV payload on fixed wings and multirotors, as they are used for photography, digitization, and reconstruction of environments (see chapter ▶ "Investigations: Accidents and Reconstructions"). The range of digital cameras available for UAVs is extensive, and devices differ greatly in resolution, cost, and weight. Drone-mounted digital cameras extend the reach of the operator allowing a new perspective of a scenario (E. M. Robinson 2016). With regard to law enforcement, this may be for surveillance or tactical support, whereas in the criminal realm, a live feed from a UAV-mounted digital camera may provide as navigation tool when smuggling drugs into a prison.

Thermal Cameras. Thermal cameras are without doubt one of the most commonly integrated payloads on current commercial systems alongside typical RGB digital cameras. For emergency first responders and law enforcement, UAV-mounted thermal cameras are increasingly used to inform decision-making and provide situational awareness when tackling a large-scale building fire or wildfire. Thermal cameras can allow operators to "see" through the smoke to better determine the location of the fire and more efficiently combat the blaze. In addition to this, these systems are also continually deployed with success when searching for a missing person, especially when searching for elderly vulnerable people often disorientated in rural areas at night.

Laser Scanners. Laser scanners or light detection and ranging (LiDAR) sensors are increasingly deployed on UAVs as a tool for 3D mapping and reconstruction (GeoSLAM 2019). Unlike camera systems, laser scanners are much better suited to map large-scale sites with improved range in comparison with camera alternative;, however, these systems are costly (usually in excess of $30,000) which has limited their uptake among law enforcement. Laser scanners are not usually integrated on commercial UAV systems unlike thermal and RGB cameras, and therefore many laser scanning systems demand specific custom UAVs for deployment.

In addition to these sensors, other popular UAV payloads include gas and temperature measurement sensors, multispectral cameras, and hyperspectral cameras. Some also have lights and speakers, as in the case of a DJI Mavic 2 Enterprise (DJI 2019b), for the purpose of communicating with an individual typically needed during a search-and-rescue mission. Consequently, UAVs may not only have one payload onboard; it is not uncommon to have both an RGB camera and a thermal camera as is the case on an Aeryon SkyRanger (Aeryon 2019) or DJI Mavic 2 Enterprise Dual (DJI 2019b). Also, in some cases, multiples of the same devices may also be used, such as when undertaking stereovision.

Criminal Drone Use and Threats to Security

All drones are designed with one of two purposes in mind, either to transport and deliver goods or as a vehicle for data capture using differing payloads and sensors. These examples, often used by businesses or law enforcement, are also true of criminal drones. The use of drone technology is currently emerging into the criminal world as cheaper commercial devices have become easier to access, modify, and use. As a result of this, over the last few years, there has been an escalation of criminal drone incidents and near-miss accidents by civilian users worldwide. The most notable criminal events include airport drone sightings, drone smuggling, potential assassination attempt, and illegal flying and illegal filming of large-scale events. Therefore, this section explores a number of incidents that have caused damage or threats to security, which in some cases have led to policy and procedural change.

Airport Sightings

Over recent years, there have been multiple drone sightings at airports all over the world. However,

mass disruption was caused at Gatwick (UK) Airport on the 19th–21st of December 2018 (BBC 2019). During this time, multiple drone sightings were reported to the police by 115 people as a drone was seen on different occasions close to the runway. Without proper procedure put into place to cope with this incident, approximately 1,000 flights were canceled or delayed as the runway was closed for a total of 33 h. Although to date, the culprit has never been caught despite extensive efforts by Sussex Police. Since this incident, Gatwick and a number of other British airports have deployed counter drone technology to cope with drone sightings better in the future. In addition to this, legislation was also altered as before this incident in the UK, there was a 1 km exclusion zone for drone use around airports without permission, which has been extended to 5 km since the event. Arguably, extending the exclusion zone may reduce the likeliness of drone sightings in the future, as a deterrent for illegal operators. However, the UAV pilot responsible for this incident was already flying within the previous 1 km exclusion zone.

Smuggling

Another example of criminal drone use that appears internationally is the use of UAV technology to smuggle drugs, phones, weapons, and other contraband into prisons. Typically these incidents involve common commercial UAV systems that have been modified to carry a desired payload of contraband into the prison (NBC News 2015). In the UK between 2016 and 2017, seven members of a gang were found to have flown £500,000 worth of drugs into prisons during 55 drone deliveries (BBC 2018a).

Assassination Attempt

During the speech of President Nicolás Maduro at a military parade in Venezuela on August 4, 2018, two drones were detonated in different locations in a possible assassination attempt of the President (BBC 2018b). Although arrests have been made, it is unclear who was behind this crime (see ▶ "Event Security" and see ▶ "Investigations: Criminal" in this encyclopedia). These systems much alike the ones outlined in section "Smuggling" appear to be modified commercial UAV systems set up to carry and detonate the explosive payloads.

Illegal Filming

In addition to these examples, other more common occurrences of illegal flying have included illegal filming of open-air area events, for example, sports events and festivals. Although the intentions of the pilot may not be malicious, overflying such a large group of people is illegal and is dangerous to the crowd in the event of a hardware failure.

Arguably, the majority of UAVs used by law enforcement and general commercial operators is likely to be reliable off-the-shelf commercial systems frequently assessed and favored for their robustness. In contrast, criminal UAVs are much more likely to be custom-built devices configured to meet the specific needs of the mission, such as a unique release mechanism for smuggling drugs (see section "Smuggling") or with the ability to remotely detonate a device as outlined in section "Assassination Attempt." With this in mind, a greater risk is generally associated with these devices than to commercially available ones as they are likely to be configured without expertise, typically using cheaper components.

In addition to the events outlined above, UAVs have been used illegally in many incidents both with and without malicious intent. For example, the use of weaponized or surveillance UAVs has been used by terror groups during acts of war overseas. Additionally, UAVs have been sighted overflying emergency events, causing a nuisance to first responders and law enforcement and potentially delaying aid being rendered to victims.

Drone Use in Law Enforcement

Much alike many other applications, UAV technology is having a profound effect upon police practice and procedure. Specially, UAVs are providing law enforcement with situational awareness and therefore offering the ability to provide an overhead view during criminal and terrorist incidents while supplying real-time information leading to an improvement in operational planning and

response, staff management, and risk assessment (see ▶ "Criminals: Terrorists" (environment, political, religious) and ▶ "Protection and security in public spaces" in this encyclopedia).

In an investigative context, aerial imagery has long been considered a valuable resource, as it can provide practitioners with aerial spatial information recorded at a specific time (Brilis et al. 2000). However, until recently, widespread access to aerial platforms by law enforcement has been limited, due to the high purchase price, operational cost, and maintenance associated with operating manned aircraft (e.g., helicopters). For this reason, the emergence of low-cost drone technology for law enforcement is providing aerial support to even the smallest departments (Robinson 2016). This is enabling many practitioners to access "real-time" remote sensing abilities, with the opportunity of rapidly overseeing large search areas using covert approaches (Pringle et al. 2012). Recent international events that have demonstrated the benefits of situational awareness provided by UAVs have included, but are not limited to, the surveying of a structure after a fire, such as the Grenfell Tower fire (London, UK) in June 2017 and the Notre Dame fire (Paris, France) in April 2019.

As such, the scope of UAV technology within law enforcement is extending rapidly as new applications are recognized daily. With this in mind, for completeness in this entry, other uses of UAV technology relevant to emergency and security management have been included although this is not an exhaustive list (West Yorkshire Police 2019; Wiltshire Police 2019):

- Searching for missing persons.
- Surveillance of VIP visits.
- Tactical operation support.
- Coordination of multiagency events.
- Crime scene recording.
- Crime scene reconstruction (see chapter ▶ "Investigations: Accidents and Reconstructions").
- Land surveying.

However, despite these overwhelmingly positive examples, law enforcement use of drones has been met with mixed reviews (Heen et al. 2017), with the majority of negative opinions regarding concerns with public privacy (Bentley 2018). Public perception of UAV use undoubtedly relies heavily on previous media coverage of UAV missions in the Middle East, as opposed to the use of small, commercial UAV systems popular among law enforcement. Unfortunately, adverse public perception of UAV use by law enforcement cannot be disregarded; instead, it has led to the development of legislation as discussed in the next section.

Drone Legislation and Public Perception

In an attempt to manage the recent surge of UAV pilots across the country, legislation has been introduced to provide guidelines and promote best practice among private, civil, and commercial users (see ▶ "Investigations: Criminal" in this encyclopedia). In the USA, the Federal Aviation Authority (FAA) regulates UAV use for hobbyists, commercial operators, and law enforcement for the purpose of ensuring a safe airspace for all users of manned and unmanned aircraft (FAA 2019c).

Currently, the legislation surrounding UAV use is continually evolving as new technologies and applications are providing a variety of challenges for policy makers. As such, an exhaustive review of drone legislation has not been included within this entry; however, very basic guidelines and legislation provided by the FAA have been included below for all UAV pilots (see FAA website, section "Getting Started"; FAA 2019b):

- Register your drone.
- Fly your drone at or below 400 f.
- Keep your drone within your line of sight.
- Be aware of FAA Airspace Restrictions.
- Respect privacy.
- Never fly near other aircraft, especially near airports.
- Never fly over groups of people, public events, or stadiums full of people.
- Never fly near emergencies such as fires or hurricane recovery efforts.

- Never fly under the influence of drugs or alcohol (FAA 2019b).

Further information and up-to-date guidance and legislation can be found on the FAA website for all UAV users, with an additional section available with extra resources for public safety and government users (FAA 2019a). It is, however, important to remember that these rules differ internationally and when wishing to fly a UAV abroad, it is essential to check the UAV laws in that country.

With regard to legislation, a crucial factor is being confident that the flight can be safely made, although this conclusion involves a general understanding of the flying area with regard to hazards and proximities to airfields. When operating a UAV safely, knowledge of the aircraft is also crucial, and this includes both the airworthiness of the device and the pilot's knowledge of controls, flight modes, flight times, and operating capabilities (i.e., wind speed, GPS).

In spite of the FAA legislation, it is not the role of the FAA to police or manage illegal UAV flying, but solely to provide legislation to ensure a safe and consistently managed airspace for all users across the country. As such, it is the responsibility of law enforcement to manage this activity and investigate where appropriate. With regard to this, the FAA has provided a number of resources to support law enforcement when tackling and handling illegal drone use.

Conclusion

To summarize, current law enforcement operations have shown a positive trend of police drone use despite public concerns regarding privacy. Because of these promising examples, it is likely that law enforcement drone use will further increase as legislation becomes clear and cohesive. However, as this entry highlights, the proliferation of drone use among law enforcement has also occurred within the criminal realm leading to breaches in security, damage, and frequently reported incidents "6 in 2014, 29 in 2015, and 70 in 2016" (Department for Transport 2017, p. 6). Because of this, increased planning and policies should be put in place to counteract rouge drones especially in security threat scenarios such as the Gatwick Airport (UK) drone incident in 2018.

Cross-References

- ▶ Criminals: Terrorists
- ▶ Event Security
- ▶ Investigations: Accidents and Reconstructions
- ▶ Investigations: Criminal
- ▶ Protection and Security in Public Spaces

References

Aeryon. (2019). SkyRanger UAS | Aeryon. Retrieved 9 Apr 2019, from https://www.aeryon.com/skyranger/

Ardupilot. (2019a). LEDs (Pixhawk) – Copter documentation. Retrieved 25 June 2019, from http://ardupilot.org/copter/docs/common-leds-pixhawk.html

Ardupilot. (2019b). Planning a Mission with waypoints and events – Copter documentation. Retrieved 25 June 2019, from http://ardupilot.org/copter/docs/common-planning-a-mission-with-waypoints-and-events.html

BBC. (2018a). Gang who flew drones carrying drugs into prisons jailed – BBC News. Retrieved 28 May 2019, from https://www.bbc.co.uk/news/uk-england-45980560

BBC. (2018b). Venezuela "drone attack": Six arrests made – BBC News. Retrieved 28 May 2019, from https://www.bbc.co.uk/news/world-latin-america-45077057

BBC. (2019). Gatwick drone attack possible inside job, say police – BBC News. Retrieved 28 May 2019, from https://www.bbc.co.uk/news/uk-47919680

Bentley, J. M. (2018). Policing the Police: Balancing the right to privacy against the beneficial use of drone technology. *Hastings Law Journal, 70*(1), 249–296. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/hastlj70&id=250&div=8&collection=journals.

Boon, M. A., Drijfhout, A. P., & Tesfamichael, S. (2017). Comparison of a fixed-wing and multi-rotor uav for environmental mapping applications: A case study. https://doi.org/10.5194/isprs-archives-XLII-2-W6-47-2017.

Brilis, G. M., Gerlach, C. L., & Van Waasbergen, R. J. (2000). Remote sensing tools assist in Environmental forensics. Part I: Traditional methods. *Journal of Environmental Forensics, 1*, 63–67. https://doi.org/10.1006/enfo.2000.0009.

Castillo, P., Muñoz Hernández, L. E., & García Gil, P. (2017). *Indoor navigation strategies for aerial autonomous systems*. Butterworth-Heinemann. Retrieved from https://www.sciencedirect.com/book/9780128051894/indoor-navigation-strategies-for-aerial-autonomous-systems

Department for Transport. (2017). *Small remotely piloted aircraft systems (drones)*. Retrieved from http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

DJI. (2019a). How to use DJI's Return to Home (RTH) Safely – DJI Guides. Retrieved 25 June 2019, from https://store.dji.com/guides/how-to-use-the-djis-return-to-home/

DJI. (2019b). Mavic 2 Enterprise – built to empower. Destined to serve – DJI. Retrieved 26 May 2019, from https://www.dji.com/uk/mavic-2-enterprise

FAA. (2019a). Public safety and government. Retrieved 28 May 2019, from https://www.faa.gov/uas/public_safety_gov/

FAA. (2019b). UAS – Getting started. Retrieved 28 May 2019, from https://www.faa.gov/uas/getting_started/

FAA. (2019c). Unmanned aircraft systems (UAS). Retrieved 28 May 2019, from https://www.faa.gov/uas/

Fahlstrom, P. G., & Gleason, T. J. (2012). *Introduction to UAV systems*. Hoboken: Wiley.

FrSky. (2019). Taranis X9D plus – FrSky – Lets you set the limits. Retrieved 25 June 2019, from https://www.frsky-rc.com/product/taranis-x9d-plus-2/

GeoSLAM. (2019). GeoSLAM – the experts in go-anywhere 3D Mobile mapping technology. Retrieved 26 May 2019, from https://geoslam.com/#

Heen, M. S., Lieberman, J. D., & Miethe, T. D. (2017). The thin blue line meets the big blue sky: Perceptions of police legitimacy and public attitudes towards aerial drones. *Criminal Justice Studies, 31*(1), 18–37. https://doi.org/10.1080/1478601X.2017.1404463.

Marshall, D. M. (2004). Dull, dirty, and dangerous: The FAA's regulatory authority over unmanned aircraft operations. *Issues in Aviation Law and Policy, 2004–2008*. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/isavialp2&id=355&div=&collection=

NBC News. (2015). Drone carrying package with drugs and blades found in Oklahoma Prison Yard. Retrieved 28 May 2019, from https://www.nbcnews.com/news/us-news/drone-carrying-package-drugs-blades-found-oklahoma-prison-yard-n452221

Pringle, J. K., Ruffell, A., Jervis, J. R., Donnelly, L., Mckinley, J., Hansen, J., … Harrison, M. (2012). The use of geoscience methods for terrestrial forensic searches. *Earth Science Reviews, 144*, 108–123. https://doi.org/10.1016/j.earscirev.2012.05.006.

Quan, Q. (2017). Basic composition. In *Introduction to multicopter design and control* (pp. 31–55). Singapore: Springer. https://doi.org/10.1007/978-981-10-3382-7_2.

Robinson, E. M. (2016). Chapter 9 – Special photography situations. In E. M. B. T.-C. S. P. (Third E. Robinson) (Ed.), *Crime scene photography* (3rd ed., pp. 455–586). San Diego: Academic. https://doi.org/10.1016/B978-0-12-802764-6.00009-X.

West Yorkshire Police. (2019). Drone support | West Yorkshire Police. Retrieved 25 June 2019, from https://www.westyorkshire.police.uk/about-us/our-departments/drone-support/drone-support

Wiltshire Police. (2019). Unmanned Aerial Vehicles (UAVs) – Wiltshire Police. Retrieved 25 June 2019, from https://www.wiltshire.police.uk/article/795/Unmanned-Aerial-Vehicles-UAVs-

Wingtra. (2019). Wingtra | Professional VTOL fixed-wing drones. Retrieved 24 May 2019, from https://wingtra.com/

Further Reading

FAA. (2019). Federal aviation administration. Retrieved 25 June 2019, from https://www.faa.gov/

Juniper, A. (2015). *The complete guide to drones: Build + choose + fly + photograph*. London: Octopus Publishing Group.

Završnik, A. (2015). *Drones and unmanned aerial systems legal and social implications for security and surveillance*. Cham: Springer.

E

Educational Institution Safety and Security

William J. Sullivan
Homeland Security, Eastern Kentucky University, College of Justice and Safety, Richmond, KY, USA

Keywords
School safety and security · Educational safety and security · Emergency management · Risk assessments

Definition

The following discussion addresses issues in school safety and security inclusive of strategies such as risk assessments and risk management principles that apply to safety and security concerns for educational institutions.

Introduction

These principles should provide the foundation for planning and prevention efforts at schools throughout the nation. Merriam Webster (2019) defines security as "the quality or state of being secure: such as freedom from danger: SAFETY, or freedom from fear or anxiety." When discussing the topic of security at educational institutions, the term security is typically accompanied with the word safety as observed in Webster's definition, since safety and security coexist in the development of plans, prevention efforts, and response actions designed to keep people and property safe. The phrase school safety and security will be used to describe protective efforts being used on school campuses inclusive of buildings, sporting and other events, arenas, and other locations and properties used and controlled by educational institutions.

Recognizing the Importance of School Safety, Security, and Preparedness

Educational institutions have the responsibility to protect the physical and psychological well-being of their students and staff. This includes the creation of positive school climates, preventing negative behaviors such as bullying and harassment, and being prepared to respond to threats such as weather emergencies, fires, and acts of violence. Effective crisis planning, prevention, response, and recovery strategies are essential for schools to meet this responsibility (Cowan et al. 2013). Currently there are over 98,000 schools in the United States providing education to students ranging from kindergarten through 12th grade (K-12) and over 7,000 institutions of higher education (NCES 2018). Although officials proclaim that protecting our nation's schools and their campus populations

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

is a priority and that significant improvements have been made towards the enhancement of safety and security, some locations simply go through the motions of preparedness. While the majority of schools report the existence of plans and policies to deal with school safety and security (NCES 2018), some schools still lack the level of effective planning and preparedness measures necessary to ensure students and staff are adequately prepared (NSBA 2017). Institutions of higher learning appear to be even less engaged in campus safety and security efforts than K-12 schools with training and lockdown drills, fire drills, and other protective measures less common. The reality is that too many campuses are grossly unprepared, and in some cases these institutions even engage in activities counterproductive to safety and security. Justifications for refusing to take protective security measures include the perception that measures create an invasion in privacy or the appearance of a prisonlike environment, and although a balance between physical and psychological security needs to exist (NASP 2013), basic security measures must be established.

Framework for Success

To be successful in the creation of a safe and secure climate, educational institutions must establish and reinforce interdisciplinary, collaborative, and cohesive approaches to safety and security supported by appropriate funding sources. The involvement of behavioral and mental health professionals, safety and security personnel, teachers and staff, other support groups, programs, and services, and the community itself must be integrated into an overall multitiered approach to ensure school safety and security is established and maintained. Educational professionals, including the American School Counselor Association, National Association of School Psychologists, National Association of Elementary School Principals, National Association of Secondary School Principals, National Association of School Resource Officers, and the School Work Association of America, agree that effective school safety and security efforts require the following:

- Executive level buy-in and proactive leadership
- The ability of educational leaders to utilize human and financial resources in a manner that best meets the needs of their school and community
- Providing a team-based framework to facilitate effective coordination of services and interventions
- Balancing the needs for physical and psychological safety
- Employing properly trained school mental health and safety professionals
- Providing relevant and ongoing professional development for all staff
- Integrating a continuum of mental health support within a multitiered system of supports
- Engaging families and community providers as meaningful partners
- Remaining grounded in the mission and purpose of schools: Teaching and learning (Cowan et al. 2013, p. 3)

School safety and security is dependent upon the successful integration of school safety and crisis management principles. This development and implementation of efforts should involve multiple phases and strategies focused upon preparedness, prevention, mitigation, response, and recovery efforts. Additionally a multi-hazard threat identification process, multi-hazard planning, and multi-agency support and response strategies should be utilized.

Personnel Involvement and Development of Strategies

Some believe the greatest risk to school safety and security could be the lack of effective strategies to address prevalent problems (Timm 2014). Security plans must focus on efforts to reduce risk, prevent loss, and prepare for emergencies. Although it is imperative that schools are prepared for active shooter/mass murder events, the preoccupation with these events may have taken away from the focus on other more prevalent threats to educational institutions and their students and

staff. Administrators must actively and continually engage in the identification and prioritization of key threats to their campuses and ensure that, at a minimum, the following basic measures are taken:

- Establish school safety and security practices and policies:

  Do not wait until an incident occurs. Identify potential risk exposures or vulnerabilities. Develop, document, and disseminate corresponding practices and policies. Train and drill staff and students, based on those policies and established response procedures.
- Continually monitor the school's culture and climate while identifying security needs:

  Identify your schools culture and climate as well as threats, issues, and stressors your students are exposed to, and routinely update to meet changes.
- Constantly improve upon efforts to prevent violence, sexual assault, bullying, harassment, and other issues:

  Schools must implement methods to identify victims and obtain information on perpetrators before issues become wide spread. Strategies should be continually improved upon to reduce violations while increasing the frequency of reporting by students and staff.
- Foster respect, develop quality relationships, and promote the importance of safety and security:

  Establishing a safe and secure educational environment is essential for the creation of an atmosphere that is conducive to learning. Safety and security personnel must be recognized as a vital part of school campus, and the establishment of quality relationships must be developed. By demonstrating mutual respect between school administrators, teachers, security personnel, and students, the foundation of these relationships can flourish creating an environment where information about potential threats to school safety and security will be shared.
- Educate staff, students, and response personnel; people are the most important part of any safety plan:

  Security measures are essential; however they can be inconvenient. Open communications and the establishment of a campus wide clear understanding of security concepts are needed. Improvements in the understanding of security procedures by staff members and age-appropriate students and their need to maintain situational awareness will not only improve upon the importance of safety and security, but also improve the ability to detect potential threats and strengthen defensive measures against those threats. Awareness improves preparedness and minimizes risk.
- Review, adapt, and update emergency procedures:

  Establish the ongoing practice of evaluating current threats, existing emergency plans, and prevention and response capabilities. This not only identifies flaws and weaknesses but also results in changes and improvements in safety and security efforts. Evaluations and updates are a never-ending cycle (Timm 2014, para. 3).

Success additionally requires the development of partnerships and the establishment of coordinated response efforts with mental health professionals, local law enforcement, EMS, other first responders, and the community itself. Fortunately, many institutions of higher learning have made considerable progress in coordinating response efforts with local responders; however, the critical need for involvement in continual training and the incorporation of drills with faculty, staff, and students is often lacking. This lack of training is problematic because individuals not only need to know what to do in emergency situations but also possess the mental and physical ability to perform the activities needed. This level of preparedness requires training where personnel physically practice the desired response procedures. These activities will increase the ability of individuals to effectively perform the desired responses during high-stress situations, when an individual's cognitive thought processes are significantly diminished. Proper preparation is essential to success.

Goal of Educational Safety and Security

Ultimately, the goal of all educational institutions should be to establish an enhanced level of security and preparedness while maintaining a positive learning environment. The question is: How can schools protect themselves from acts of violence, crimes, disasters, and other situations which can be harmful to students and staff and disruptive to education? No single solution exists, and approaches will vary between locations; however, the answer can best be found in a holistic, multifaceted approach that utilizes layers of security supported by effective procedures and situational awareness. Efforts must additionally include the state of individual preparedness.

Security in Layers

Effective security requires a layered approach incorporating the use of teachers and staff in primary and auxiliary security roles while employing multiple physical and physiological impediments for deterring, denying, and delaying entry or unapproved access of individuals and other threats. This holds true regardless of the type of man-made threat, whether it is a cyber threat, a thief, a sexual predator, or an armed intruder. Although deterring or preventing attacks is the primary goal, auxiliary goals include delaying intruders long enough to allow detection, response, and apprehension, thus preventing them from reaching their target or minimizing the negative impact. Potentially beneficial impediments include signs, presence of personnel, lights, locks, sensors and alarms, fences, walls, security doors, security glass, bollards, and large planters. Natural barriers such as rivers, lakes, mountains, cliffs, ditches, mature trees, and even dense vegetation can also be effective for creating physical and/or physiological security barriers. Generally speaking the more layers of effective security, the better the result.

Since it is impossible to make a location or asset completely secure, a common strategy in security, often referred to as target hardening, involves expanding the use of protective measures to enhance security and decrease the criminal's chance of success or perceived chance. Creating a location that appears to be more secure than similar locations enhances security efforts and theoretically deters the adversary from attacking the more secure site in favor of another less secure location where the attack is more likely to succeed.

Effective Use of Technology

The use of technology to identify potential threats can be crucial. For example, cyberattacks may go undetected for substantial periods of time, and individuals in active shooter incidents are often initially unaware of the attack. Shot sensors with automated notification systems can be an effective solution for ensuring occupants and law enforcement are quickly notified about active shooter situations. This technology is additionally capable of providing accurate locations of gunfire and continual updates to authorities.

Other technologies include intrusion resistant doors, windows, bullet-resistant glass/panels, and automated locking mechanisms which can quickly lock doors creating barriers and denying access or mitigating the impact of violence to potential victims. The use of closed circuit television (CCTV) enhanced with threat detection software can improve the identification of suspicious activity and unauthorized entry. The use of hard rooms which are bullet and intrusion resistant and equipped with CCTV monitors and unpublished communications lines allows occupants the ability to establish and maintain communications with first responders, security personnel, and others in the school. Another potentially beneficial technology is software that allows officials to scan social media for potential threats/concerns associated with cyber bullying, suicidal discussions, threats of violence, or other harmful activities. The software flags troublesome posts that can be reviewed by preselected officers and/or school officials trained to identify language associated with likely threats. Although this technology can be controversial, by explaining the intentions of the search, the fact that only public communications are examined, and the narrow focus of the search, concerns can be reduced.

Prevention

The ultimate goal of safety and security is to avoid the loss of life and property through the prevention or interruption of actions before they cause harm. To effectively accomplish this, one must first identify potential threats. Critical information about threats to schools often comes from within the school itself or the greater community. Obtaining information about impending threats can be challenging and is often dependent on the development of trust between individuals before information will be shared. This trust is best achieved by fostering positive relationships between officials, students, and the community at large. After information concerning potential threats is obtained, it can be evaluated and prioritized through the use of risk assessments/threat assessments. These risk assessments, along with the use of emergency management and security principles, can be effective in the development of strategies to prevent or reduce harmful activities.

Deterrence

Deterrence is a desirable outcome that can be achieved by making a location appear so secure from attack or other unlawful activities that a successful attempt seems unlikely or significantly less likely than at another more vulnerable location. Even though no single solution exists for all locations, successful security programs should incorporate the use of multiple physical and physiological impediments to aid in the identification and deterrence of individuals, vehicles, and other threats.

Deny or Delay Access

Although budgets, school culture and climate, and even the physical locations themselves and their surroundings will impact what can incorporated into protective measures, one should consider the use of beneficial impediments such as security personnel, lights, fences, walls, protective bollards, large decorative planters, and natural barriers. By denying or even delaying access, security can improve its ability to detect adversaries and prevent the infliction of harm or at least mitigate the negative consequences of the breach regardless if the attempt involves a cyber threat or an armed intruder. If the threat involves active shooters or other violent individuals, the act of simply closing and locking the doors of classrooms during instructional periods is an effective and often simple means of denying or delaying access to students and staff. There have not been any successful breaches by active shooters into classrooms with securely locked doors.

Identifying and Preparing for Threats

School safety is a relatively new area of study that has been brought to the forefront by repeated cases of violence, including active shooter situations (Borum et al. 2010; Cornell and Mayer 2010). The ensuing rise in media coverage and public concern has resulted in significant changes in school discipline and school safety measures throughout the nation (Borum et al. 2010). In reality, the percentages of violence-related deaths occurring at schools are extremely small, while the frequency in victimizations of students and staff at schools is considerable.

The Centers for Disease Control and Prevention (CDC) stated that homicide is the second leading cause of death among youth aged 5–18; however, only between 1% and 2% of these deaths happened on school grounds or on the way to or from school (2018). The CDC further reported that between 1992 and 2015, the number of homicides of students 5–18 years old at schools or coming to and from schools averaged 22.8 per year, and the number of suicides averaged 5.9 (2018). However, the *Indicators of School Crime and Safety Report* provided by the National Center for Education Statistics (NCES) stated that during the 2015–2016 school year, 79% of public schools recorded one or more incidents of violence, theft, or other crimes had taken place, amounting to 1.4 million crimes (2018). During the same school year, 47% of schools reported one or more of the crimes to the police, resulting in a total of 449,000 crimes. Ten percent of public school teachers reported being threatened with injury by a student from their school, and 6% reported that a student from their school had physically attacked them. In 2015, approximately 3% of students aged 12–18 reported that they were afraid of being attacked or harmed at

school during the school year and 22% of students in grades 9–12 reported that illegal drugs were made available to them on school property (NCES 2018). The report further indicated that many of these crimes were not reported to law enforcement including serious violent crimes, where only half of the cases were reported to police. Serious violent crimes included "rape, sexual assault other than rape, physical attack or fight with a weapon, threat of physical attack with a weapon, and robbery with or without a weapon" (NCES 2018, p. 55).

Risk Management and Risk Assessments

Schools and universities must identify, evaluate, and prioritize their threats and associated risks and then develop effective strategies to manage those risks. This process should begin with the use of risk management strategies and include the incorporation of risk assessments. The Department of Homeland Security defines risk management as "the process for identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken" (2013, p. 7). Although one typically thinks of security in relation to man-made threats against persons or property, security personnel are involved in the prevention, mitigation, preparation, response, and recovery efforts for all threats, man-made and natural regardless of the cause. Risk management is intended to enhance the overall decision-making process, increase the ability to achieve objectives, and shape and control risk.

Although risk management cannot identify or eliminate all risk through the incorporation of risk assessments, the process can prioritize the risk identified and guide safety and security efforts towards the threats and associated vulnerabilities that are most likely to result in significant harm. This process will allow schools, federal, state, and local officials the ability to identify, develop, and employ approaches that are effective in preventing or mitigating future incidents. Risk management additionally incorporates the use of sound organizational practices such as planning, preparedness, program evaluation, and process improvement while considering existing budgetary restraints. According to DHS (2013), the key principles for effective risk management include:

1. Unity of Effort: Risk management is an enterprise-wide process and should promote integration and synchronization with entities that share responsibility for managing risks.
2. Transparency: Risk management depends on open and direct communications.
3. Adaptability: Risk management actions, strategies, and processes should remain dynamic and responsive to change.
4. Practicality: Risk management cannot eliminate all uncertainty nor is it reasonable to expect it to identify all risks and their likelihood and consequences.
5. Customization: Risk management programs should be tailored to match the needs and culture of the organization while maintaining balance with the specific decision environment they support (pp. 11, 12).

Risk Management Process

In an effort to ensure uniform, systematic and interoperable approaches to risk management, DHS encourages the use of a standardized process. Standardization improves the ability of different agencies and entities to work effectively together while possessing a shared understanding of information, analysis, and an improved and informed decision-making process. One should keep the aforementioned risk management principles in mind when implementing the risk management process.

The DHS risk management process includes:

1. Defining and framing the context of decisions and related goals and objectives
2. Identifying the risks associated with the goals and objectives
3. Analyzing and assessing the identified risks
4. Developing alternative actions for managing the risks and creating opportunities and analyzing the costs and benefits of those alternatives

5. Making a decision among alternatives and implementing that decision
6. Monitoring the implemented decision and comparing observed and expected effects to help influence subsequent risk management alternatives and decision (2013, pp. 15–25)

To develop effective strategies, officials must examine realistic threats while also taking into consideration the individual school and property, surrounding environment, and the school's climate and culture. This should be accomplished through the use of risk assessments and/or school assessments.

Risk Assessments and the Development of Site-Specific Strategies

Most educational institutions have experienced substantial cuts in budgets, and all institutions have finite resources. A critical element in the creation of a safe and secure environment for educational facilities and campuses is the identification and prioritization of threats and associated risk. This can be effectively accomplished through the use of assessments typically referred to as risk assessments. Risk assessments allow officials to prioritize potential threats, illegal, or harmful activities by considering the likelihood of events occurring in association with the negative consequences that would result if they did occur.

There are numerous methodologies that have been used to evaluate risk. These methodologies significantly range in complexity from the basic risk matrix developed by the Department of Homeland Security in 2007 ($R = T \times V \times C$) which evaluates risk through the examination of threats, existing vulnerabilities, and the resulting consequences to more complex models that expand upon the CARVER matrix, which historically was used by US Special Forces for mission planning. The CARVER matrix examines the areas of Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability to evaluate risk. There are also methodologies designed to focus on one specific threat area such as the *Operational Guide for Preventing Targeted School Violence* published by the United States Secret Service in cooperation with the US Department of Homeland Security.

It is important to identify a risk assessment methodology that meets the needs of the institution but does not exceed the capabilities of the assessors, information available, or other resources needed. Assessments should not be conducted by a single individual or randomly chosen personnel. Assessments should be completed by a team of carefully selected assessors from multiple backgrounds and disciplines that are applicable to the needs of the assessment. For example, it would be appropriate for an assessment focused on school violence to include carefully selected educational professionals (teachers, councilors, administrators, etc.), law enforcement, behavioral and mental health professionals, social services, and other disciplines/entities (NASP 2017). Team members should also receive appropriate training prior to conducting the assessments.

Common Threats to Schools, Universities, and Their Associated Campuses

When examining the existence of threats and associated risk, there are obviously varying factors and concerns impacting educational institutions such as the age of the students, size and population of the campus, physical structure and design of buildings and public spaces, assets present, existing security measures, and even external threats associated with the region. Regional and local variables for consideration include population density, crime rates, visibility of school, ease of access, regional weather associated threats, or even exposure to potential external threats such as chemicals or other harmful materials located in nearby plants or being transported on highways or railways. Exposure to pandemics and other public health hazards must be considered along with a host of other external and internal threats. Even the type of educational institution significantly impacts safety and security measures. Many of the issues facing high school students are not prevalent in the lower elementary grades, for example, the use of illegal drugs in high schools versus grade schools. Logically this results in differences in the strategies and use of resources for combating illegal drug in the two types of schools. The National Center for

Education Statistics reported that only 5.9% of public grade schools conducted random sweeps using drug detection dogs, while 62.3% of public high schools used these tactics (NCES 2018).

Middle schools and university campuses certainly have their own priorities as well, resulting in varying approaches. Although differences in prioritization of threats exist between institutions, there are also common concerns that many institutions share. Examples include bullying and cyberbullying; physical and sexual assault/abuse; verbal and other communicated threats; possession of weapons, drugs, alcohol, or other prohibited items; theft, criminal mischief, and other property crimes; cyber intrusions; fire; threats from nature such as tornados, hurricanes, winter storms, floods, tsunamis, and earthquakes; pandemics and the spread of disease; mental health issues; and even litigation. One of the most common concerns addressed is violence or the threat of violence, including the statistically small but devastating threat of active shooters/mass murders.

Active Shooters/Mass Murders

There are various attack methods that have been used in active shooter/mass murder events including firearms, knives or other cutting instruments, blunt striking weapons, explosives, and even vehicles. The type of weapons, funding available, and a host of other variables, can impact the measures used by schools against such weapons, and schools must carefully take these factors into account when developing plans and protective measures. If a school is attempting to prevent vehicles from gaining access to areas on campus frequently used by pedestrians, the use of trees, ditches, walls, bollards, and large planters could be an effective and unobtrusive tactic. However, shortfalls in funding can make these measures cost prohibitive to implement throughout the entire campus. Therefore planners should consider identifying areas commonly associated with dense populations and make those locations the priority for implementation of these protective measures.

If the goal is to keep potential attackers out of a classroom, educational institutions can replace existing doors with doors that are capable of being automatically and remotely locked or update existing doors with automated door locks. Although it is an expensive improvement, especially when a school is updating all doors, it would enable doors to be locked without delay when an armed intruder was detected and a lockdown was initiated. However, another simple, less costly, and potentially more effective means to reduce risk would involve not waiting until a lock down was called to secure and lock classroom doors but to manually close and lock classroom doors at the beginning of each class and keep them locked until the instructional period is over. By closing and locking classroom doors during instructional periods, the level of risk will be effectively reduced and safety significantly improved. This simple tactic would effectively minimize or eliminate existing shortcomings resulting from delays in notifications and the time and danger involved for teachers attempting to reach, close, and lock their doors. This method will additionally negate the issues stemming from a teacher's inability to lock doors because of their loss of cognitive thought and diminished fine motor skills resulting from exposure to extreme stress. This approach obviously depends on the ability for rooms to be locked while still allowing students to exit in the event of a fire or other emergency requiring evacuation. In situations where evacuation is warranted, hallways should be briefly checked for threats before students exit the classroom and before students enter adjoining hallways.

Although this is a simple and effective tactic, many educators remain reluctant to incorporate these types of tactics claiming it is too disruptive to open doors for late students. Such excuses are not acceptable. If educators are not physically capable of opening the door for latecomers, assistants or age appropriate able-bodied students can be used. Educators should additionally keep classroom keys in their possession at all times and/or memorize codes for entry in the event a door becomes locked, and they need to reenter the classroom. Doors which are either unable to be locked and secured or which will not allow

students to exit when the door is locked should be replaced or updated with the appropriate hardware. If all educational institutions that have fallen victim to active shooter attacks had effectively implemented and practiced the policy of closing and locking doors during class periods and checking hallways before evacuations, the number of lives saved would have been significant. The Sandy Hook Advisory Commission reported that there has never been an active shooter who successfully breached and entered a closed and locked classroom door.

Participants in Preparedness

In reality, everyone has a role in enhancing their security by maintaining situational awareness of their surroundings and through the development of personal response plans (mental rehearsals). Personal response plans should outline primary and alternate plans of action in the event an active shooter or other critical incident occurs. Response plans should include options such as immediate and rapid evacuation of the threat area, involving the identification of primary and secondary escape routes prior to the emergency. An alternate tactic in active shooter situations should involve remaining out of sight, preferably in a secure area that provides barriers capable of stopping gunfire, should be considered. A last resort response in active shooter/mass murder situations may involve the aggressive use of force against the assailant. This defensive tactic can include the use of improvised weapons such as fire extinguishers to disorient attackers and/or the use other available items to physically assault the attacker. As another last means of defense, age and physically capable groups that are sheltered within a room or other area can develop coordinated response plans that involve the use aggressive physical force to protect themselves in the event an assailant gains entry into their area. These plans should include identifying specific duties/tasks for each of the key defenders and a coordinated overall plan of action. Each member should mentally rehearse and prepare for their duties. These aggressive tactics are certainly dangerous but a better option for physically capable individuals than relying on the hope that they will be spared.

Conclusion

Clearly the involvement and participation of faculty, staff, and students are essential to success. However, the incorporation of security engineering and protective design along with the development and implementation of effective plans, policies, and procedures is also essential. Training is another key component and should include the initial and ongoing instruction of personnel while also considering the use of age and situational appropriate activities that reinforce and engrain concepts introduced in training. The use of drills and scenarios can be effective in improving personnel's ability to perform tasks while under stress, when their cognitive thought process is significantly diminished. Success is also dependent upon the establishment of partnerships including the development of coordinated response efforts with local law enforcement and other first responders. Each of these actions is not possible without the support of administration and key officials, making administrative buy-in essential to success.

The process may sound complicated, but in reality it is a logical progression for any safety and security professional. Being prepared will save lives in active shooter situations and other critical incidents, and local law enforcement and other emergency responders can be an excellent resource for the development of safety and security measures. Ultimately it is the responsibility of educational institutions to provide a safe environment that is conducive to learning. To effectively achieve this, teachers, students, and staff must become involved in safety and security efforts and knowledgeable about response strategies and their respective roles. Personnel and age-appropriate students must maintain situational awareness and should develop personal plans (mental rehearsals) outlining primary and alternate plans of action they will take in the event of an active shooter or other critical incident. These steps will

reduce hesitation to act, which can be fatal during critical incidents. Personal action plans should include options such as the immediate evacuation of the threat area or remaining out of sight, preferably in a secure area that provides cover capable of stopping gunfire. Mental preparation should additionally include consideration for the use of aggressive force against the shooter. It is also critical for students, parents, school personnel, and the community to challenge educational institutions that are not properly prepared. Lives may depend on it.

References

Borum, R., Cornell, D., Modzeleski, W., & Jimerson, S. R. (2010). What can be done about school shootings: A review of the evidence. *Educational Researcher, 39*, 27–37.

Centers for Disease Control and Prevention (CDC). (2018). School associated violent death study. Retrieved from https://www.cdc.gov/violenceprevention/youthviolence/schoolviolence/savd.html

Cornell, D., & Mayer, M. (2010). Why does school order and safety matter? *Educational Researcher, 39*, 7–15.

Cowan, K. C., Vallancourt, K., Rossen, E., & Pollitt, K. (2013). *A framework for safe and successful schools [Brief]*. Bethesda: National Association of School Psychologists.

Department of Homeland Security (DHS). (2013) Risk management fundamentals. Retrieved from https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf

Merriam Webster (2019). Retrieved from https://www.merriam-webster.com/dictionary/security

National Association of School Psychologists (NASP). (2013). A framework for safe and successful schools. Retrieved from http://www.nasponline.org/resources/framework-safe-and-successful-schools.aspx.

National Association of School Psychologists (NASP). (2017). *Policy recommendations for implementing the framework for safe and successful schools. [Brief]*. Bethesda: National Association of School Psychologists.

National Center for Education Statistics (NCES). (2018). Indicators of school crime and safety: 2017. Retrieved from https://nces.ed.gov/pubs2018/2018036.pdf.

National School Boards Association (NSBA). (2017). Trending in school security. Retrieved from https://www.nsba.org/newsroom/american-school-board-journal/asbj-august-2017/trending-school-security

Timm, P. (2014). Six strategies to address the most pervasive problems plaguing our schools: Elsevier. Retrieved from https://www.elsevier.com/connect/guns-are-not-the-biggest-threat-to-schools

Emergency Management: Best Practices

Bernard A. Jones
Division of Criminal Justice, Legal Studies and Homeland Security, College of Professional Studies, St. John's University, Jamaica, NY, USA

Keywords

All-hazards approach · Business continuity · Emergency notification system (ENS) · Emergency operations center (EOC) · Hazard mitigation · Incident Command System (ICS) · Mass notification system (MNS) · Mitigation · Mutual aid agreements · Preparedness · Recovery · Response

Definition

Emergency management is defined as the process which involves the ability to mitigate, prepare for, respond to, and recover from emergencies, crises, and/or disasters.

Introduction

Since the beginning of recorded history, disasters have occurred, and there is no person, community, or organization immune to the adverse impacts of disasters. Unfortunately, when disasters occur, there is a general lack of proper preparedness, response, and recovery actions and capabilities, even when the hazards are chronic and frequent. When a natural disaster does occur, people, communities, and organizations respond vigorously to address the negative impacts caused by the event. Additionally, the hope is that the same vigor displayed during a response to an emergency is also evident during lessons learned meetings to help reduce the possible damage from any future disasters. Research has shown that immediately following recovery from a disaster, there is a sense of normalcy, translating into a sharp increase in thoughts and

behaviors *away* from the disaster event. The notion that we have "survived" takes over, and any ill feelings about the disaster subside. Disasters affect people, communities, and organizations in many different and adverse ways.

People, communities, and organizations must remain steadfast in the various phases of emergency management to allow for the best possible outcome regarding any future disasters. The range and variety of emergencies that could potentially involve emergency management is quite extensive. It is, therefore, undeniable and essential that emergency management is an integral part of daily lives. Four phases or functions of emergency management exist: preparedness, response, recovery, and mitigation. This chapter focuses on describing emergency management best practices and providing examples within each four phases or functions of emergency management.

Emergency Management: Preparedness

Emergency management preparedness is defined as a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action regarding disasters. A critical element within emergency management preparedness is the development of an emergency management response or action plan. As with every response or action plan, the plan is only as good as the degree by which it is reviewed, approved, tested, and communicated.

Preparedness also entails performing the required degree of due diligence regarding the understanding of the threat landscape. This aspect of preparedness is essential as it places focus on those threats which are most prevalent and assists with the development and refinement of the emergency management response or action plan. Preparedness also focuses on preparing for both natural and human-made disasters.

Emergency management preparedness measures provide a heightened standard or "pre-disaster" awareness and structure from catastrophe. The risk of injury, loss of life, or damage of operational capabilities is limited with proper emergency management, crisis communication, business continuity, and evacuation plans. Primarily, emergency management preparedness focuses on the needed readiness to respond to all-hazards incidents and emergencies. Because emergency and disaster events can occur without notice, people, communities, and organizations engage in emergency management preparedness to help establish an enhanced state of readiness to facilitate response. Emergency management preparedness best practices include, but are not limited to:

- Mandating and conducting, at a minimum, annual emergency management plan testing, review, and update, or whenever there has been a change in the organization that can impact the plan (e.g., significant staffing changes, changes in services offered, etc.). Akin to conducting fire and evacuation drills, mandating and executing the testing of emergency management plans is an essential component of practicing sound emergency management and a best practice.
- Coordinating and conducting testing and reviews of emergency management plans with external entities (e.g., local first responder organizations, regional organizations, and other company locations and facilities) that are critical to the ongoing operation of the organization. Whether human-made or natural, disasters can cause catastrophic damage; therefore, partnering with critical external entities pre-disaster has proven to serve as a fundamental best practice.
- Periodically conducting awareness training activities that helps ingrain preparedness within the culture of the home, community, and organization. Research has shown that people, communities, and organizations that regularly conduct awareness training activities are more prepared for responding to disasters. In addition to awareness activities, it is also a best practice to periodically coordinate scheduled awareness training in coordination with regularly scheduled plan testing efforts. A best practice would be to conduct

awareness training as part of the regular emergency management plan review and testing initiatives.
- Adopting an all-hazards risk management approach by conducting an organizational hazard identification and risk assessment allowing organizations to identify their vulnerabilities concerning managing disaster and emergencies. It is essential for people, communities, and organizations to not only perform risk assessments for natural disasters like severe weather but also to practice sound risk management with an all-hazards approach (e.g., including both natural and human-made disasters).
- Instructing emergency management personnel to complete training in the use of the Incident Command System (ICS). The ICS encompasses a standard approach to emergency management and can significantly enhance emergency management response by identifying a defined set of roles and responsibilities. Disasters inherently can be complicated to respond to, because of different factors and impacts which can change rapidly. When there is a framework already defined, established, and tested regarding roles and responsibilities, emergency managers are better prepared to address the twists and turns that complex disasters can bring.
- Including processes and protocols which address communication in emergency management preparedness. The magnitude and importance of clear, accurate, and timely communication within emergency management cannot be understated. A critical best practice is to create a communication plan which includes establishing protocols for notifying family members, members of the community, and individuals within the organization, prior, during, and after disaster and emergencies. The emergency management communication plan helps establish external communication processes to allow a family, community, and organization to keep abreast of response to disasters and emergencies.
- Addressing additional emergency-related strategies, including shelter-in-place, evacuation, fire drill, and lockdown plans, and reviewing and testing them periodically.
- Establishing mutual aid/assistance agreements with external stakeholders. This best practice is one that has successfully been implemented and well documented during large-scale disaster events like Hurricane Katrina and Superstorm Sandy. A crucial task within preparedness is to conduct periodic reviews and update mutual aid/assistance agreements as required.
- Incorporating infants and young children, as well as pets, in emergency management planning activities. The welfare of infants and young children, as well as pets, is an essential component of emergency management preparedness and often overlooked (see ▶ "Emergency Management: Infant and Young Children Feeding in Emergencies" chapters in this volume).

Emergency Management: Response

Emergency management response entails how people, communities, and organizations react to crises and disaster events. The emergency management response phase encompasses the coordination and deployment of resources to address the crisis or disaster to minimize harmful impacts. Emergency management response best practices include, but are not limited to:

- Utilizing the ICS framework and capability during the response phase. The ICS framework significantly enhances response by providing a defined structure regarding roles and responsibilities during emergency response.
- Utilizing and leveraging the established communication plan created as part of preparedness activities during the response to an emergency.
- Adopting, testing, and integrating an emergency notification system (ENS) or mass

notification system (MNS). An ENS or MNS is defined as a tool or application which sends one-way messages to inform the public of an emergency. Organizations best served by an ENS or MNS include fire and local law enforcement; emergency management organizations; federal, state, and local governments; cities and communities; and building owners, building management companies, and businesses that can justify its need and investment. ENS and MNS significantly improve the safety and security of an organization by providing alerts and real-time instruction during an emergency or disaster. ENS and MNS have been in existence for a brief number of years and are commonplace within academic institutions. These systems are often also referred to as "reverse 911" communication systems.

- Utilizing pre-established emergency operations center (EOC) process, plan, and capability. While not a viable option for individuals or families, the implementation of an EOC enables communities and organizations to respond effectively to large-scale disasters.

Best Practices: Emergency Management – Recovery

The emergency management recovery phase consists of those activities that continue beyond the emergency management response phase to manage stabilization efforts. "Recovery involves providing immediate support during the early post-disaster period necessary to return vital life-support systems to minimum operational levels and continuing to provide support until the community returns to normal" (Petak 1985).

Although recovery is a distinct phase in the life cycle of emergency management, activities that take place during other phases can affect the recovery phase.

The recovery phase begins immediately after the threat to human life has subsided. The goal of the recovery phase is to bring the affected area back to some degree of normalcy (see also ► "Emergency Management: Recovery" in this volume). Emergency management recovery best practices include, but are not limited to:

- Engaging in research concerning financial funding from disaster relief sources and organizations. Disaster relief sources and organizations exist to provide needed assistance and relief during the recovery phase.
- Establishing travel and lodging agreements near recovery locations. Among the four emergency management phases, it is the recovery phase that inherently has the most extended duration, as the impacts from a disaster may require reconstruction of buildings, roads, and infrastructure, which takes time to complete. By establishing travel and lodging agreements ahead of an emergency, employees are in a better position to focus efforts on recovery operations.
- Engaging human resources within the organization's emergency management plan to allow the department to assist during the recovery phase. Establishing employee safety and travel kits and creating cash accounts with debit cards are excellent best practices regarding emergency management recovery activities.
- Engaging the community at large in establishing partnerships before disaster events.

Best Practices: Emergency Management – Mitigation

Emergency management mitigation is an effort to reduce the loss of life and property by lessening the impact of disasters and emergencies. Mitigation involves structural and non-structural measures taken to limit the effects of disasters and emergencies. Emergency management mitigation actions, involving physical structures, include changing the characteristics of buildings or the environment. Examples would consist of flood control projects, raising building

elevations, and clearing areas around structures. Emergency management non-structural components would entail adopting or changing building codes. Overall, the importance and interest in conducting hazard mitigation have grown recently in response to the increase in both the frequency and severity of natural and human-made disasters, which unfortunately have resulted in the loss of life and property and economic losses. Hazard mitigation is "any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster event" (FEMA 1996). Emergency management mitigation best practices include, but are not limited to:

- Initiating hazard mitigation activities at the city, local, and community level, where land-use decisions are made, as well as construction codes and standards adopted and enforced. Also, hazard mitigation efforts at the community level provide an opportunity for community leaders to incorporate hazard mitigation into their decision-making processes (see also ▶ "Natural Hazards" in this volume).
- Incorporating hazard mitigation techniques into decisions. Hazard mitigation can be as simple as conducting periodic tree trimming near company facilities and homes. This mitigation best practice can ensure that severe weather events that may cause tree branches to snap would not impact power lines or homes from damage. As a best practice, promoting and investing in hazard mitigation efforts is a direct way that families, businesses, and communities can reduce human and economic losses from future disasters.
- Expanding the ability to minimize the impact of a future emergency or disaster. This best practice was tested and implemented during global pandemic fears in recent years.
- Collaborating and partnering with an organization's jurisdiction to create mitigation plans that address the community's unique risks, reduce vulnerabilities, and enhance community resilience. Collaboration efforts also enable a community to maintain a "local perspective" to the mitigation plan and create "community buy-in." Taking the collaboration best practice a step further, it is also essential to consider developing a collaborative planning approach. The approach encompasses establishing a multi-jurisdictional planning team, pooling resources, and expertise from the community, using in-house staff, and effectively involving the public in hazard mitigation planning.
- Taking advantage of funding through grants. These funding sources can be used in hazard mitigation efforts and activities.
- Including counter-terrorism awareness and training which is a modern-day best practice and can significantly minimize or mitigate the impacts of future domestic terrorist attacks (see also ▶ "Terrorism: Domestic" in this volume).
- Implementing a comprehensive cybersecurity policy to help mitigate the impacts of future cyberattacks (see also ▶ "Cybersecurity: Policy" in this volume).

Conclusion

There is no doubt that disasters will continue to be a part of human existence, causing adverse impacts on people, communities, and organizations throughout history. Over time both human-made and natural disasters have caused devastation in the form of loss of life, severe property damage, substantial financial ruin, and destruction to critical infrastructure. The discipline of emergency management provides a comprehensive approach to management efforts before, during, and after disasters occur. It provides the framework and structure to enhance the ability of people, communities, and organizations to address disasters and continues to evolve with changes in hazards, technology, and the environment. The four foundational phases or functions of emergency management include preparedness,

response, recovery, and mitigation. Each emergency management phase differs concerning scope, objectives, and purpose, but together all four aspects work to address the management of disasters. The different phases of emergency management, while each independent, work along a continuum or cycle. Unfortunately, some people, communities, and organizations do not implement emergency management best practices. These best practices have been identified and shared to benefit people, communities, and organizations alike. Those who implement emergency management best practices significantly enhance their ability to address future human-made and natural disasters.

Cross-References

- ▶ Cybersecurity: Policy
- ▶ Emergency Management: Infant and Young Children Feeding in Emergencies
- ▶ Emergency Management: Pets
- ▶ Emergency Management: Recovery
- ▶ Natural Hazards
- ▶ Terrorism: Domestic

References

Federal Emergency Management Agency. (1996). *Guide for all-hazard emergency operations*. Washington, DC: FEMA. Retrieved from https://www.fema.gov/pdf/plan/slg101.pdf

Petak, W. (1985). Emergency management: A challenge to public administration. *Public Administration Review, 45*(Special issue), 3–7.

Further Reading

Canton, L. (2007). *Emergency management: Concepts and strategies for effective programs* (p. 2007). Hoboken: Wiley.

Haddow, G., Bullock, J., & Coppola, D. (2017). *Introduction to emergency management* (2nd ed.). Burlington: Butterworth-Heinemann.

Phillips, B., Neal, D., & Webb, G. (2012). *Introduction to emergency management* (pp. 178–181). Boca Raton: CRC Press.

Szwejczewski, M. (2008). Best practice. In C. L. Cooper (Ed.), *The Blackwell encyclopedia of management*. Malden: Blackwell Publishing.

Emergency Management: Crisis Communication

Marlies Sas[1], Wim Hardyns[2,3], Koen Ponnet[4,3] and Genserik Reniers[5,3]
[1]Research group on Law Enforcement and Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Antwerp, Belgium
[2]Institute for International Research on Criminal Policy (IRCP), Ghent University, Ghent, Belgium
[3]Antwerp Research Group on Safety and Security (ARGoSS), University of Antwerp, Antwerp, Belgium
[4]Department Communication Sciences, imec-mict-Ghent University, Ghent, Belgium
[5]Safety and Security Science Group, TU Delft, Delft, The Netherlands

Keywords
Crisis communication · Risk communication · Crisis event · Crisis management · Social media

Definition

A crisis situation is "a major occurrence with a potentially negative outcome affecting the organization, company, or industry, as well as its publics, products, services, or good name" (Fearn-Banks 2016, p. 1).

Crisis communication can be specified as "the collection, processing, and dissemination of information required to address a crisis situation" (Coombs 2010, p. 20).

Introduction

In recent years, crisis communication has become one of the major areas of interest in crisis management literature. Authors agree that it is impossible to manage a crisis adequately without including communication in the crisis management process. Crises or threats for crises

create an environment where information is needed. Numerous researchers explored various crisis response strategies depending on the nature of crisis and the crisis phase. This major interest has created an abundant amount of information for experts working on crisis management practices (Coombs 2010).

It is almost impossible to list all possible crises for organizations. Events such as explosions, activist actions, rumors, fire, earthquakes, death, product harm, terrorism, and strikes are threats that could evolve in a crisis situation (Coombs 2007). Although these crises occur in various forms, numerous authors have developed crisis typologies based on overlapping characteristics (Mitroff et al. 1996; Lerbinger 1997). Coombs (2007) synthesized these typologies into 11 crisis types: operational disruptions from disasters, workplace violence, rumors, unexpected loss of key leadership, malevolence, challenges, technical-error accidents, technical-error product harm, human-error accidents, human-error product harm, and organizational misdeeds.

While communication has often been seen as the most efficient way to improve the management of these crisis, two communication strategies, risk communication and crisis communication, have tended to focus on different stages in the crisis management cycle. Traditionally associated with public health and emergency management traditions, it is the aim of risk communication to inform people about potential harm in order to encourage them to take action to mitigate the risk. Risk management holds the assumption that the public has the right to know possible dangers. Transparency about potential harm allows people to make informed choices regarding risk (Seeger 2006). While risk messages mainly emerge before a crisis situation occurs, crisis communication, which has its roots in crisis management and public relations, focuses on communication during and after an event. Communicators are focused on the actions that must be done in order to resolve or contain the crisis by spreading well-timed, accurate, and useful information. Despite the differences between these types of communication, they are both part of the larger business continuity management plans of an organization (Coombs 2010).

Theoretical Frameworks in Crisis Communication

Several theoretical frameworks have been developed for the understanding of communication processes and results in crisis situations. While some researchers rely on related disciplines such as sociology, psychology, and rhetoric, several studies make a contribution to crisis communication research by applying public relations theories. For example, according to the contingency theory of strategic conflict management (Cameron et al. 2007), various contingency factors can affect the communication between the organization and the public. The theory seeks to select the most appropriate crisis response depending on the threat level of the crisis. Crisis communicators can draw on the issue management theory (Ulmer et al. 2007) when attempting to understand the public perceptions and attitudes toward an organization during a crisis event. Grunig's (Grunig 1997) situational theory of publics defines that various specific factors can be identified in the responses of the public toward an organization in a crisis situation. The theory explains how people communicate and when communication aimed at the public is most effective depending on the phase of the crisis event. The apologia theory of Fearn-Banks (2016) focusses on defending the organization's reputation and protecting the image after the organization has been accused of a misdeed. Aside from a real apology, the theory includes denial, explanation, and expressing sorrow as crisis communication strategies. Building on the apologia theory, the image restoration theory (Benoit 1995), or later referred to as the image repair theory, identifies two components of an attack to the image of an organization: the attacked person or organization is responsible for the action and the action has to be considered offensive. The perception of the crisis is fundamental to image restoration. Benoit (1995) identifies five possible response strategies: (1) denial, when the organization denies that the act occurred; (2) evading responsibility, which can contain provocation, defeasibility, making excuses, and suggesting the action was justified based on good intentions; (3) reducing

offensiveness, when the organization attempts to reduce the negative feelings experienced by the audience; (4) corrective action, when the organization claims that the problem will be corrected; and (5) mortification, when the organization admits responsibility and asks for forgiveness.

Today, the more recent situational crisis communication theory (SCCT) of Coombs (2007) accounts for the majority of studies on crisis communication management. It has its roots in Weiner's attribution theory (1985) and presents an overview of different response strategies to specific crises. Similar to the image repair theory, Coombs emphasizes on the responsibility of the crisis and the impact of communication on the general perception of the action. More important than the actions itself is the perception of the crisis (Benoit 1995; Coombs 2007). Depending on the responsibility of the organization, three clusters of crises are categorized: (1) victim crises, such as terrorism or natural disasters where the organization has little or no responsibility; (2) accident crises, such as technical errors, where the organization can be partly held responsible; and (3) intentional crises, such as fraud, where the organization could have prevented the crisis. Possible response strategies involve the denial of the crisis, the diminish of the crisis or the focus on rebuilding the relationship with the stakeholders, including bolstering as secondary response strategies.

The dominant crisis communication theories above do not address how social media can be used in crisis management. Although the use of social media during crisis events has become a vibrant and rapidly growing interest of researchers in recent years. To establish a framework for the use of social media as a crisis communication tool, the social-mediated crisis communication model (SMCC) (Jin et al. 2011) was developed. According to this model, three key publics transmit crisis information: (1) influential social media creators who create social media messages, (2) social media followers who consume the information spread by the social media creators, and (3) social media inactives who may consume crisis information indirectly via mouth-of-mouth communication or traditional media. Organizations have to take into account five factors (crisis type, crisis origin, organizational infrastructure, crisis message source, and crisis message form) when communicating about the crisis. Depending on those factors, different perceptions of the messages by the intended public can be explained (Jin et al. 2011).

Communication Within the Three Phases of Crisis Management

In order to approach the crisis in an effective way, communication starts long before an event occurs and continues after the immediate threat has receded. In literature, authors identified three phases of a crisis situation: pre-crisis, crisis and post-crisis. In the pre-crisis phase, or the developmental stage, conditions which can lead to a crisis accumulate. When the primary impact of a crisis event is experienced, the crisis stage is reached. A triggering event, such as an accident, outlines the start of this phase. The post-crisis phase is characterized by recovery and self-assessment which may reveal future opportunities or negative effects (Meyer and Reniers 2016). The length of each phase depends merely on the complexity of the situation, the emerged issues, and the time needed for resolution (Ray 1999).

All crisis phases, from the pre-crisis prevention period to the actual crisis and post-crisis containment, must be covered by specific communication strategies. A variety of types of crisis communication can be identified depending on the phase of the event (Coombs 2010). Equally for all crisis phases, the involvement of a broad number of stakeholders is recognized. This implies that any individual or group who receives an impact of the achievement of the organization's objectives has to be included in the crisis communication management (Ulmer et al. 2007). Based on the work of Coombs (2010), specific types of communication can be identified depending on the crisis phase. Below we outline these types.

Pre-crisis Phase

In the pre-crisis phase, the crisis communication plan includes preventive measures that reduce the

known risks that could potentially lead to a crisis situation and presents an overview of the preparatory activities for management during the crisis. At this moment, information required to address a crisis situation has to be collected, decisions about how to manage potential crises have to be made, and people who will be involved in the management process of the crisis have to be trained. Communicators have the responsibility to create awareness about potential crises in order to encourage the public to be heedful for possible crisis sources. As it is a challenge to not normally accept the changes or anomalies as regular or innocent, pre-crisis communication is focused on the identification of risks or irregular signals and the education of the public about the preparation for a crisis situation (Seeger 2006).

Crisis Phase

During the crisis, communication is crucial since it has a significant effect on the outcome of the crisis. During the event, information needed by the crisis team is collected and processed, and messages to people outside of the crisis team are created and disseminated. The crisis response guidelines for messages toward the public highlight three focal characteristics: quickness, accurateness, and consistency. First, the initial response has to be provided immediately after the crisis situation occurred. It is important that the responsible crisis communicator has the possibility to tell his side of the story before the media or other relevant actors start sharing their often inaccurate information. Second, messages have to be updated regularly in order to focus on sharing only accurate information with the outside world. Third, crisis communication has to be consistent. A recommended communication strategy is the appointment of a crisis team that shares the same information with the responsible communicators in order to maintain accuracy (Coombs 2010).

Post-crisis Phase

In post-crisis phase, communicators stop focusing on managing the crisis itself but concentrate on the effects of the situation. If during the event communicators promised to share specific information afterward, this is the moment of delivering on that promise. Breaking the promise could result in the public losing their trust in the capacity of handling future emergency situations. Additionally, communicators share available information about the recovery process, corrective actions, or results of investigations of the crisis. The quantity of messages depends on the promised information during the event and the length of the post-crisis phase. Finally, post-crisis stage provides an opportunity to evaluate the operations of the organization, including the circumstances that led to the crisis and the used crisis management strategy (Mitroff et al. 1996).

Best Practices in Crisis Communication

In order to support crisis professionals with creating a communication plan adapted to the crisis phases, researchers of the National Center for Food Protection and Defense (NCFPD), a US Department of Homeland Security Center of Excellence, created a list of best practices in crisis communication based on evaluations of multiple case studies and an exhaustive review of literature about this topic (Seeger 2006). Numerous communication scholars and practitioners contributed to the compilation of the practices, which were published in a special issue on risk and crisis communication in the *Journal of Applied Communication Research* (2006). In later years, these best practices have been tested and expanded in several scientific publications (e.g., Sellnow et al. 2009; Veil and Ojeda 2010). In total, ten best practices were identified:

1. *The establishment of process approaches and policies*. While communication is often seen as an important factor after a risk or crisis occurred, the description of the different phases of a crisis event above already showed that communication should be involved in decisions before, during, and after an emergency situation. By integrating communication strategies in the decision process, communication issues can be solved more immediately and more fully in the planning and response phase of a crisis. Activities such

as the education of the public should be part of the ongoing policy of the preparedness for emergency situations.

2. *Pre-event planning*. In order to make the crisis management process effective, crisis planning and risk analysis are indispensable. Preventive actions such as the identification of potential threats, the calculation of needed resources, the synchronization of internal and external communication processes, and the assignment of responsibilities for team members make the approach of the crisis situation more efficient. Additionally, it is important that the crisis communication plan contains structures for regularly updates and revisions.
3. *Partnerships with the public*. Since the public has the right to know what risks it faces, they should be considered as a legitimate and equal partner in crisis management. During a crisis, it is the responsibility of the crisis team to share knowledge about the event with the public. The audience can, vice versa, also provide essential information that can be useful to mitigate the crisis. Thus, a dialogical approach between the public and the crisis management team is suggested.
4. *Attention for the public's concerns and understanding of the audience*. In order to create a dialogue between the public and the crisis team, it is important that the concerns of the public are taken into account regardless of whether the perceived risk is manifested. When positive relationships and a reservoir of goodwill are established before a crisis situation, the approach of a crisis event will be more successful.
5. *Honest, candor, and open communication*. By sharing information openly and honestly before, during, and after a crisis, the risk of reducing the trust of the public can be avoided. Once the public considers the organization no longer as a source of trustworthy information, the efficiency of crisis management is strongly reduced.
6. *Collaboration and coordination with credible sources*. In addition to the establishment of a strong dialogue with the public, the creation of strategic partnerships with credible sources is considered as a best practice. This network consists of reliable people who are indispensable for the coordination of crisis messages and activities. Authors emphasize the need of finding relevant partners at all levels and creating relationships before a crisis occurs.
7. *Meeting the needs of the media and remaining accessible*. In many cases, the media is the only source from which the public can gain information about the crisis situation. Meeting the needs of the media and remaining accessible is necessary in order to transfer the right messages. When communicating with the media, inconsistency should always be avoided. Therefore, media training for crisis managers and communicators should be part of the pre-crisis planning.
8. *Communication with compassion, concern, and empathy.* It is important that communicators react with compassion, concern, and empathy when referring to the crisis situation. Showing an expression of genuine concern and empathy convinces the public of the legitimacy and appropriateness of the proposed actions. Human reactions will always be better received.
9. *Acceptance of uncertainty and ambiguity.* Crisis situations always contain some level of uncertainty. Communicators could choose to wait until all relevant information is available before sending out messages. Hence, accepting uncertainty and ambiguity encourages the release of quick and truthful messages. A best practice is considered to acknowledge that the given information is still uncertain, for example, with statements as "we do not yet have all the facts." On the one hand, this allows the communicator to refine the message when more details about the crisis situation become clear, while on the other hand, statements that are likely to be shown as inaccurate are avoided.
10. *Messages of self-efficacy.* Messages that contain suggestions about what people could do to reduce the harm promote self-efficacy. The content of these messages depend on the nature of the event and can differ from avoiding certain products to donating in

order to help others. It is important that the public understands why a certain action is suggested and considered as meaningful.

Sellnow and Vidoloff (2009) added an eleventh best practice to the list of the NCFPD: the acknowledgement and account for cultural differences. It is important that those who do have a limited access to mainstream media still got informed about the crisis situation. Communicators should include the use of specific channels to reach underrepresented populations in their communication plan.

Based on these guidelines, communication professionals can improve their communication management plan. The eleven best practices are the principles or processes forming the basis of an effective crisis communication approach. It is important to mention that those best practices often complement each other and function together. As every crisis is a unique event that can evolve in very different directions, the establishment of a well-integrated and situation-specific approach is suggested (Seeger 2006).

Incorporating Social Media in Crisis Communication

Recently, social networking technologies have become a new trend in crisis communication management. During all stages of crisis events, people make use of multiple communication channels to reduce uncertainty and to obtain a sense of personal control over the situation (Lin et al. 2016). Because its convenience and quick accessibility, the use of social media during crisis events is increasing. In emergency situations worldwide, they have generated both opportunities and concerns (Branicki and Agyei 2015).

Firstly, social media have the opportunity to inform a wide audience about their safety and prosperity in a very short time period. Updates about the crisis event can be shared and reshared within a couple of seconds, reaching millions of people (Veil et al. 2011). Secondly, by regarding social media as a crisis communication channel, a more direct and personal connection with the public can be set up. The community becomes part of the actual crisis communication response (Lin et al. 2016). Thirdly, it allows crisis teams to get real-time information from the audience. By using social media proactively, comprehensive information from observers can be collected directly. Individuals have the ability to become sources of information by sharing their opinions and experiences with others. It provides clarity about the publics crisis needs as concerns and questions can immediately be addressed (Branicki and Agyei 2015). Finally, social media can be used to get in contact with less reachable individuals. By implementing various social network technologies in the crisis communication plan, individuals who cannot be reached by mainstream media could be informed through social media about the crisis situation (Veil et al. 2011).

On the other hand, while social media facilitates the relationship with the public during the crisis event, it can increase the organization's vulnerability as it is almost impossible to control the high-speed spread of information through this medium. Therefore, crisis communicators should manifest receptiveness, integrity, and fair-mindedness to hold back the public from being convinced of less-reliable sources of information. In order to do so, communicators should share a considerable amount of information through social media before a crisis situation occurs to guarantee that information seekers could already identify the reliable sources. When doing so, they will consult the information sources they know and have confidence during the crisis situation (Lin et al. 2016). Subsequently, since anyone with a social media account has the ability to share information or give reactions on other messages, the possibility of the spread of misinformation increases. Therefore, it is important to monitor all crisis-related posts. When trusted sources are unable to provide enough information, other individuals can start rumoring because of the lack of information. The impact of this misinformation cannot be underestimated for the reputation and future of the organization (Lin et al. 2016). Finally, concerns are rising about the possible technology failures when using social media. It is important that the use of social media is fully integrated in the crisis management and approaches. This implies that social media

technologies have to be tested and that evolvements in this field have to be followed up accurately in order to regularly update the crisis communication plan (Veil et al. 2011).

Despite these concerns, communicators almost have no choice in using social media as the public is already making use of it when informing each other about crises. In recent years, new media have acted as the main communication channel during crisis events. People are taking pictures or turn to the internet to get information and share opinions. If crisis communicators decide to narrow their focus on traditional media channels, conversations about the crisis will go on through social media without the organization's voice being heard. Importantly, literature shows that new and social media technology should not replace but complement the traditional communication channels (Schultz et al. 2011).

Conclusion

This article presented an up-to-date overview of the available literature about crisis communication in emergency and crisis situations. The overview has shown that the topic has been of great interest of numerous researchers. With the emerging use of social media, new opportunities and concerns have risen. In the future, more new emerging technologies in crisis management such as drones or virtual reality could create interesting opportunities and carefulness. As most relevant crisis communication approaches and practices were presented, this overview could be used by crisis communicators when making their crisis management plan of business continuity plan more effective.

Cross-References

- ▶ Emergency Management: Evacuations
- ▶ Emergency Management: Recovery
- ▶ Geographic Information Systems (GIS) Applications in Emergency Management
- ▶ Public-Private Partnerships: Security Organizations

References

Benoit, W. L. (1995). *Accounts, excuses and apologies: A theory of image repair strategies*. Albany: State University of New York Press.

Branicki, L. J., & Agyei, D. A. (2015). Unpacking the impacts of social media upon crisis communication and City evacuation. In J. Preston, J. Binner, T. Galla, N. Jones, J. King, M. Kolokitha, & M. Smyrnakis (Eds.), *City evacuations: An interdisciplinary approach*. Berlin/Heidelberg: Springer.

Cameron, G. T., Pang, A., & Jin, Y. (2007). Contingency theory: Strategic management of conflict in public relations. In T. Hansen-Horn & B. Neff (Eds.), *Public relations: From theory to practice*. Boston: Pearson Allyn & Bacon.

Coombs, W. T. (2007). *Ongoing crisis communication: Planning, managing and responding*. Thousand Oaks: Sage.

Coombs, W. T. (2010). Parameters for crisis communication. In W. T. Coombs & J. Holladay (Eds.), *The handbook of crisis communication*. Chichester: Blackwell Publishing.

Fearn-Banks, K. (2016). *Crisis communications. A casebook approach*. New York: Routledge.

Grunig, J. E. (1997). A situational theory of publics: conceptual history, recent challenges and new research. *Public Relations Research: An International Perspective, 3*(48), 3–46.

Jin, Y., Liu, B. F., & Austin, L. L. (2011). Examining the role of social media in effective crisis management: The effect of crisis origin, information form, and source on public's crisis responses. *Communication Research, 41*(1), 74–94.

Lerbinger, O. (1997). *The crisis manager: Facing risk and responsibility*. Mahwah: Lawrence Erlbaum Associates.

Lin, X., Spence, P. R., Sellnow, T. L., & Lachlan, K. A. (2016). Crisis communication, learning and responding: Best practices in social media. *Computers in Human Behavior, 65*, 601–605.

Meyer, T., & Reniers, G. L. L. (2016). *Engineering risk management*. Berlin: De Gruyter.

Mitroff, I. I., Pearson, C. M., & Harrington, L. K. (1996). *The essential guide to managing corporate crises: A step-by-step handbook for surviving major catastrophes*. New York: Oxford University Press.

Ray, S. J. (1999). *Strategic communication in crisis management: Lessons from the airline industry*. Connecticut: Quorum Books.

Schultz, F., Utz, S., & Göritz, A. (2011). Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media. *Public Relations Review, 37*, 20–27.

Seeger, M. W. (2006). Best practices in crisis communication: An expert panel process. *Journal of Applied Communication Research, 34*(3), 232–244.

Sellnow, T. L., & Vidoloff, K. G. (2009). Getting communication right. *Food Technology, 63*(9), 40–45.

Sellnow, T. L., Ulmer, R. R., Seeger, M. W., & Littlefield, R. S. (Eds.). (2009). *Effective risk communication: A message-centered approach*. New York: Springer.
Ulmer, R., Sellnow, T., & Seeger, M. (2007). *Effective crisis communication. Moving from crisis to opportunity*. Thousand Oaks: Sage.
Veil, S. R., & Ojeda, F. (2010). Establishing media partnerships in crisis response. *Communication Studies, 61*(4), 412–429.
Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A work-in-process literature review: Incorporating social media in risk and crisis communication. *Journal of Contingencies & Crisis Management, 19*(2), 111–122.

Further Reading

Coombs, W. T., & Holladay, J. (Eds.). (2010). *The handbook of crisis communication*. Chichester: Blackwell.
Fearn-Banks, K. (2016). *Crisis communications. A casebook approach*. New York: Routledge.
White, C. M. (2011). *Social media, crisis communication, and emergency management*. Boca Raton: CRC Press.

Emergency Management: Crisis Management and Response

Michael K. Lindell
Department of Urban Design and Planning, Institute for Hazards Mitigation Planning and Research, University of Washington, Seattle, WA, USA

Keywords
Emergency response functions · Incident Command System · Multiorganizational networks

Definition

A community crisis is a potentially overwhelming situation that requires an urgent response to avoid severe consequences that exceed a community's capability to absorb. Often its cause, effects, and means of resolution are ambiguous (Pearson and Clair 1998) because of its unpredictability, speed of onset, and scope and duration of impacts (Perry 2018). These event characteristics produce a sense of uncertainty and urgency as households, organizations, and government agencies seek to rapidly mobilize and deploy available response resources.

Introduction

Community crises typically threaten both physical (casualties, damage to buildings, infrastructure, and agriculture) and social (psychosocial, sociodemographic, economic, and political) impacts (Lindell 2013, 2019; NRC 2006a). These potential impacts create agent-generated demands for actions to limit or avoid these impacts and response-generated demands for actions to coordinate all of the individuals and organizations that are responding to the agent-generated demands. Crisis response activities are conducted during a time period that begins with the detection of the event. In some cases, such as hurricanes, hazard monitoring systems (satellite detection coupled with computer-based atmospheric forecast models) ensure authorities are promptly alerted to hazard onset, so there is a long period of time to activate an emergency response organization. In other cases, such as earthquakes, preimpact prediction is usually not available, but prompt assessment of the impact area is feasible within a matter of minutes to hours. This allows emergency managers to direct search and rescue resources to extricate victims from collapsed structures. The crisis response ends when the situation is stabilized, which means that the risk of loss of life and property has returned to pre-crisis levels.

Emergency Response Functions

FEMA (1998, p. 12) described the goal of emergency response as "to save lives and property by positioning emergency equipment and supplies; evacuating potential victims; providing food, water, shelter and medical care to those in need; and restoring critical public services." More broadly, Lindell and Perry (1992) summarized emergency planning guidance in USNRC (1980)

and NRT (1987) in terms of four basic functions that emergency responders must perform in responding to disaster demands: emergency assessment, hazard operations, population protection, and incident management. These four functions provide a succinct way of describing what response organizations must do as they respond to an emergency. The purpose of *emergency assessment* is to define the nature and magnitude of the event by evaluating conditions in the physical and social environments. In the case of a hazardous materials transportation incident, this would involve identifying the types and quantities of chemicals involved, the current and forecast meteorological conditions that determine the direction and distance of exposure hazard, and the extent to which the population at risk has sheltered in-place or evacuated.

Hazard operations consist of preventive and corrective actions that limit either the likelihood or the magnitude of hazard impacts. These actions do so either by controlling the source (e.g., plugging leaks in hazmat containers) or by limiting hazard impacts (e.g., placing sandbags around structures threatened by floods). Hazard operations actions are preventive if they avoid a release to the environment. For example, spraying water on a tank car of chlorine that is next to a burning tank car of propane will prevent the chlorine from expanding and rupturing its tank (Noll and Hildebrand 2012). Hazard operations actions are corrective if they reduce the magnitude or terminate a release in progress (e.g., plugging a leaking tank car). Other hazard operations actions avoid property exposure by protecting or strengthening building envelopes (putting up shutters before a hurricane or shutting doors and windows and turning off HVAC systems before a toxic chemical release), securing building contents (e.g., in anticipation of earthquake aftershocks), or turning off utilities (to prevent escaping gas from being ignited by downed power lines).

Population protection actions range from the use of protective gear by responders to evacuations by community residents. The preferred method of population protection is to prevent people from being exposed to the hazard. This can be accomplished by initiating evacuation or sheltering in-place for people inside a hazard zone and access control to prevent people outside a hazard zone from entering it. If people have been exposed, emergency managers can reduce consequences such as the severity of injury or probability of death by conducting search and rescue operations to locate and extricate victims. Once this has been done, medical actions can be initiated such as first aid, transport to medical facilities, and definitive care.

Incident management ensures that emergency assessment, hazard operations, and population protection actions are undertaken in a timely and effective manner and that emergency responders have sufficient resources to do their jobs. In addition, it involves coordinating with other organizations to acquire additional resources and providing public information about the incident to people who do not need to take protective action.

As Table 1 indicates, the four basic functions have subfunctions that are similar to those that FEMA's (2010) CPG-101 recommends as functional annexes to the Basic Plan of a jurisdiction's Emergency Operations Plan (EOP). As the table indicates, FEMA's list of recommended functional annexes (which is more comprehensive than in earlier versions of this guidance such as DCPA 1978, and FEMA 1990) does not explicitly address emergency assessment or the initial activation of emergency response agencies, facilities, and equipment.

The interrelationships among these functions can be seen in Fig. 1, which Lindell et al. (2006) adapted from an earlier version in Lindell and Perry (1992). An emergency is defined by a *chain of events* beginning with an actual (or potential) release of energy or hazardous material that is currently being (or will in the near future be) transmitted through the environment to a community. The hazard agent acts together with community characteristics and environmental conditions to threaten exposures of persons and property (indicated by the solid lines). In turn, these exposures will produce physical (casualties, damage to buildings, infrastructure, and agriculture) and social (psychosocial, sociodemographic, economic, and political) impacts. To avoid these impacts, emergency managers use the information available at different stages of the chain of events

Emergency Management: Crisis Management and Response, Table 1 Typologies of emergency response functions (Adapted from Lindell et al. 2006)

Organizational functions	Organizational subfunctions	NRT-1 functions	CPG-101 local plan functional annexes	ICS sections
Emergency assessment				
	Threat detection/ emergency classification	Ongoing incident assessment		
	Hazard/ environmental monitoring	Ongoing incident assessment		Planning
	Population monitoring and assessment			
	Damage assessment		Damage assessment	Planning
Hazard operations				
	Hazard source control	Containment and cleanup	Firefighting; oil/hazmat response	Operations
	Protection works	Public works		Operations
	Building construction			
	Contents protection			
			Energy; agriculture and natural resources	
Population protection				
	Protective action selection		Population protection	
	Population warning	Warning systems and emergency public notification	Warning	
	Protective action implementation	Personal protection of citizens	Transportation	
	Impact zone access control/ security	Law enforcement	Public safety and security	
	Reception/care of victims	Human services	Mass care, emergency assistance, housing and human services	
	Search and rescue	Fire and rescue	Search and rescue	Operations
	Emergency medical care	Health and medical	Public health and medical services	
	Hazard exposure control	Response personnel safety	Worker safety and health	Command
Incident management				
	Agency notification/ mobilization	Initial notification of response agencies		

(continued)

Emergency Management: Crisis Management and Response, Table 1 (continued)

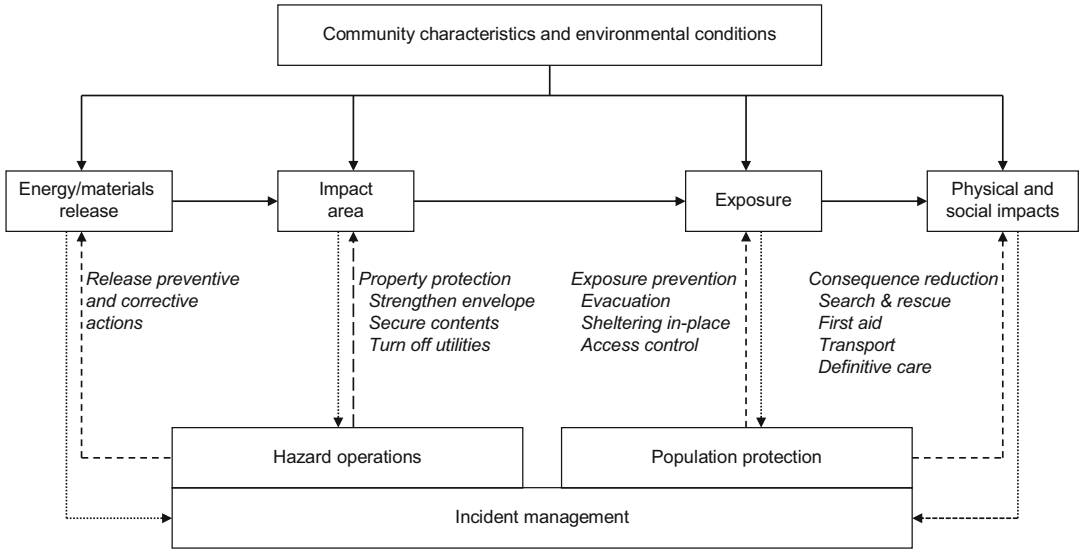
Organizational functions	Organizational subfunctions	NRT-1 functions	CPG-101 local plan functional annexes	ICS sections
	Mobilization of emergency facilities & equipment			Planning
	Communication/ documentation	Responder communications	Communications	All sections
	Analysis/ Planning			Planning
	Internal direction and control	Direction and control	Direction, control, and coordination	Command
	Public information	Public information/ Community relations	External affairs/emergency public information	Command
	Finance/ administration	Resource management	Financial management	Finance/ administration
	Logistics		Resource management; Logistics management and resource support; volunteer and donations management	Logistics
	External coordination	Direction and control	Mutual aid/multijurisdictional coordination; private sector coordination; long-term recovery	Command

to perform emergency assessment actions (indicated by the dotted lines) that allow them to assess the threat, impact area, exposure, and potential impacts. If incident managers can project future disaster demands (i.e., later stages in the chain of events) from current conditions, they can anticipate the tasks that will need to be performed at that later time (indicated by the dshed lines). In turn, this allows them to request additional resources and deploy them before they are needed rather than when it is too late.

Emergency Response Organizations

Effective incident management requires local emergency response organizations to rapidly mobilize human and material resources. This, in turn, requires a predetermined *concept of operations*, which is a summary statement of what emergency response functions are to be performed and how they are to be accomplished. In almost every case, this requires advance planning for coordination across a variety of local public sector, private sector, and nongovernmental organizations. It also requires a strategy for mobilizing extra-community resources and integrating them into the emergency response. Such coordination requires agreement about the emergency functions to be performed, as well as assignment of responsibility for emergency function performance to local and external organizations. In addition, the organizational structure must be defined in terms of the title and duties of each of the positions within the emergency response system and the reporting relationships among these positions.

Emergency response activities are usually accomplished through the efforts of diverse groups – some professional, others voluntary. In most rapid onset incidents such as earthquakes, the first people to respond are uninjured survivors in the impact area who begin the task of search and rescue. These volunteers are followed by local professionals such as police, firefighters, emergency medical services personnel, and public works employees. However, some components of the population protection function are assigned to other organizations. Mass care is usually



Emergency Management: Crisis Management and Response, Fig. 1 Chain of events model. (Adapted from Lindell et al. 2006)

assigned to the American Red Cross or Salvation Army, and evacuation support is often assigned to local transit authorities or school districts.

According to Dynes (1970), *established* organizations respond by performing their normal tasks with their normal staff, *extending* organizations perform new tasks with their normal staff, *expanding* organizations perform their normal tasks with new staff, and *emergent* organizations perform new tasks with new staff. When the agent-generated demands exceed the capacities of individual organizations, an *emergent multiorganizational network* (Drabek et al. 1981) forms to coordinate the response with the objective of achieving mutual goals as completely as possible with a minimum of performance gaps, unnecessary duplication, confusion, or conflict (Gillespie 1991). However, focusing on response-generated demands such as improvised coordinating mechanisms necessarily diverts valuable time from the performance of agent-generated demands such as search and rescue, so a *planned multiorganizational network* is a more effective way to achieve crisis management goals (Lutz and Lindell 2008).

Another response-generated demand is the acquisition of a wide variety of resources that are needed to ensure there will be an adequate emergency response. These resources include:

- *Trained staff* in sufficient numbers of personnel in each job title and their organization into cohesive response teams that have standardized titles and job descriptions so they can understand each other's capabilities and limitations,
- An *Emergency Operations Plan (EOP)*, *Standard Operating Procedures* (SOPs), and other job aids to guide emergency responders in performing tasks that are critical, infrequent, and difficult to perform,
- *Equipment* for emergency assessment (e.g., toxic gas monitoring devices), hazard operations (ranging from tank patching equipment to bulldozers and sandbags), population protection (ranging from respirators to traffic barricades), and incident management (e.g., computers, cell phones, and radios).
- *Facilities* such as incident command posts (ICPs), staging areas, incident bases, camps for emergency responders; jurisdictional

emergency operations centers (EOCs) to coordinate *inter*-agency activities, departmental operations centers (DOCs) to coordinate *intra*-agency activities, joint information centers (JICs), and congregate care centers ("public shelters") to house evacuees.

A major challenge is to ensure that each responding organization has timely access to the resources that it needs. In major disasters, this requires inventories of emergency response resources within the affected jurisdiction and adjacent jurisdictions, as well as preincident agreements authorizing the release of those resources, and effective communications procedures for requesting them during an incident.

The Incident Command System (ICS)

Southern California fire departments recognized the need for a common structure for emergency response organizations in the aftermath of their experience during the 1970 wildfires (Auf der Heide 1989). At that time, emergency responders were impeded by disparate organizational structures, inadequate emergency assessments, poorly coordinated planning, uncoordinated resource allocation, and inadequate inter-agency communications. This situation was consistent with the findings of five decades of research on organizational response to disasters, which repeatedly found that major disasters require coordinated response by many organizations. In many cases, much valuable time that should have been devoted to an incident's agent-generated demands was lost to its response-generated demands – trying to overcome differences in organizational design, positional titles, emergency response training, and organizational procedures (Drabek 1986; Lindell and Perry 1980; NRC 2006b).

The lack of standardization in the design of emergency response organizations was not an accident. For many years, the federal government provided state and local governments with criteria for evaluating their EOPs (DCPA 1978; FEMA 1990). However, it avoided requiring a specific structure for emergency response organizations. This resulted in a proliferation of organizational structures, positional titles, resource names, and operational procedures that impeded interjurisdictional cooperation – even among identical emergency response agencies (e.g., fire departments) from neighboring jurisdictions.

In the aftermath of the 1970 wildfires, Southern California firefighters developed a system that evolved into the Incident Command System, which was guided by a few basic principles (FEMA 2004). First, all jurisdictions use a common organizational structure defined by standardized names and functions for subunits and standardized names and duties for individual positions (standardization). Second, a division of labor assigns each unit a specific function to perform (functional specificity). Third, subunits are established to limit the number of personnel directly supervised by each unit manager (manageable span of control). This is usually five subordinates but can range from three to seven. Fourth, personnel from a given professional discipline, such as police or fire, are assigned to the same unit in the emergency response organization (unit integrity). This facilitates teamwork and also simplifies recordkeeping. Fifth, most incidents are managed by a single Incident Commander (IC) but a Unified Command (UC) team manages the emergency response when multiple agencies have statutory authority and responsibility for a specific type of incident. Sixth, emergency responders develop Incident Action Plans (IAPs) that include specific, measurable objectives and evaluate their effectiveness by monitoring the achievement of these objectives (management by objectives). Seventh, the IC or the UC team allocates all resources – personnel, facilities, vehicles, and equipment – to emergency response tasks (comprehensive resource management).

These features make the ICS a flexible structure for assembling resources and directing emergency response units that is adaptable to all types of hazards. Moreover, ICS can address large, complex, multijurisdictional incidents as effectively as very small, routine incidents. The modular organization of ICS allows an emergency

response organization's size and composition to change as the IC activates only those functional units needed to address current and projected incident demands. The Command Section oversees four sections – Planning, Operations, Logistics, and Finance/Administration – that are staffed as appropriate to incident conditions. Section chiefs work with Command staff to formulate an emergency response strategy and then direct tactical operations that are implemented by specialized branches within each of the four sections. In a fully implemented ICS, branches are established under sections to implement the tactical operations they have been assigned. Sectors are defined beneath branches and execute specific tasks. For large incidents, sections can be subdivided into geographic or functional branches which, in turn, are divided into geographical divisions or functional groups. Lower levels of organization include task forces comprising different resources and strike teams composed of a single type of resource.

In larger incidents, the Incident Commander is supported by a Safety Officer, a Public Information Officer (PIO), and a Liaison officer to coordinate with agencies such as law enforcement and the EOC. Within the ICS structure, Command delegates responsibility for implementing its emergency response strategy to the four section chiefs. The Operations Section deals directly with all hazard source control activities at the incident scene. These activities include terminating hazardous materials releases; suppressing fires; extricating, triaging, and transporting victims. The Planning Section is charged primarily with collecting, analyzing, and distributing incident data, forecasting resource demands, and other planning functions. The Logistics Section supports the emergency response organization by providing needed resources (e.g., facilities and equipment) and services (communications, information technology, medical). The Administration Section focuses on procurement, cost recovery, liability, and risk management.

After establishing an Incident Command Post to direct on-scene operations, the Incident Commander should follow the Emergency Operations Plan's concept of operations by assigning emergency response functions to the government agencies or other community organizations that are responsible for performing each of them. In addition, the emergency response organization should develop an IAP for each operational period that identifies the incident objectives, unit assignments, a communications plan, a medical plan, a safety plan, and other specialized plans or information, as needed. The IAP might be oral for a small incident but should utilize ICS forms to produce written documentation for major incidents. The IAP should be based upon situation reports (SITREPs) that describe the incident status and the resource status. SITREPs should address essential elements of information (EEIs) such as hazard information, incident boundaries, environmental information, and hazard impacts.

In any major emergency, the emergency response organization will need to maintain constant contact with the jurisdictional EOC, which will provide policy guidance and continuous technical assistance to responders at the incident scene. Such support includes obtaining weather forecasts, coordinating warning and evacuation, supervising mass care facilities, and disseminating public information. Moreover, an EOC is needed to request extra-community resources and to direct their disposition as they arrive from other local jurisdictions and higher levels of government.

Research on ICS Implementation

Although it seems logical to assume that implementing the basic principles of ICS will yield more effective incident management, there have been limited tests of this assumption. One line of evaluation has been to examine the merits of ICS on purely theoretical grounds or on the basis of anecdotal data (see Drabek and McEntire 2002, and Jensen and Thompson 2016, for reviews of articles of this type). For example, one early criticism of ICS was that it ignored the role of volunteers (Wenger et al. 1990), an issue that has been addressed is subsequent guidance (FEMA 2017). Moreover, as Table 1 indicates,

one disadvantage of ICS is that it largely ignores the population protection function, probably because these activities are usually performed away from the incident scene. Current versions of ICS must address these activities within the Operations Section or assume that they are being directed from the EOC, as was the case in Hurricane Rita (Lutz and Lindell 2008).

More generally, there is little empirical research on ICS effectiveness. A few studies have reported some degree of success in ICS implementation but noted that such success depends on each participating organization's extensive training and routine utilization of this system. Such high levels of training and utilization are feasible for organizations such as police, fire, and emergency medical services agencies whose missions to respond to routine emergencies. However, routine utilization of ICS is implausible for agencies such as Public Health and Social Services and even frequent training on ICS would be a significant burden on these organizations. Thus, even the limited research on ICS reveals limitations that need to be addressed; additional empirical tests of ICS effectiveness are needed to determine if there are other deficiencies (Boersma et al. 2014; Jensen and Thompson 2016).

Conclusions

The ICS's flexible structure can make three significant contributions to emergency response operations (Lindell et al. 2006). First, standardization can facilitate first responder training because training materials can be readily shared across jurisdictions. Second, ICS can increase the reliability of emergency response operations because its comprehensive structure can decrease the likelihood that important functions will be overlooked in the heat of emergency response. Third, ICS replaces *emergent multiorganizational networks* with *planned multiorganizational networks*. This avoids time delays associated with lengthy assessments of other response agencies' capabilities and the development of mutually agreed procedures. However, the fundamental basis of ICS is a set of management principles whose validity has been documented in research on *established* organizations that perform their normal tasks with their normal staff under modest levels of uncertainty and urgency. The unanswered question is whether these principles also apply to *extending*, *expanding*, and *emergent* organizations. Practitioner experience suggests that the *planned multiorganizational networks* established within ICS are superior to *emergent multiorganizational networks*. Nonetheless, there have been flaws found in ICS implementation. Consequently, further research is needed to assess ICS effectiveness in a wider range of conditions and identify modifications that can make it more effective.

Cross-References

- ▶ Emergency Management: Evacuations
- ▶ Emergency Management: Preparedness and Planning
- ▶ Emergency Management: Shelter in-Place

Acknowledgments This research was supported by the National Science Foundation under Grants CMMI-1760766 and CMMI-1826455. None of the conclusions expressed here necessarily reflects views other than those of the author.

References

Auf der Heide, E. (1989). *Disaster response: Principles of preparation and coordination*. St. Louis: Mosby. Available at orgmail2.coe-dmha.org/dr/Images/Main.swf.

Boersma, F. K., Comfort, L. K., Groenendaal, J., & Wolbers, J. J. (2014). Incident command systems: A dynamic tension among goals, rules and practice. *Journal of Contingencies and Crisis Management, 22*(1), 1–4.

DCPA—Defense Civil Preparedness Agency. (1978). *Standards for local civil preparedness*. Washington, DC: DCPA—Defense Civil Preparedness Agency.

Drabek, T. E. (1986). *Human system responses to disaster: An inventory of sociological findings*. New York: Springer-Verlag.

Drabek, T. E., & McEntire, D. A. (2002). Emergent phenomena and multiorganizational coordination in disasters: Lessons from the research literature. *International Journal of Mass Emergencies and Disasters, 20*(2), 197–224.

Drabek, T. E., Tamminga, H. L., Kilijanek, T. S., & Adams, C. R. (1981). *Managing multiorganizational emergency responses*. Boulder: University of Colorado Institute of Behavioral Science.

Dynes, R. (1970). *Organized behavior in disaster*. Lexington: Heath-Lexington Books.

FEMA—Federal Emergency Management Agency. (1990). *Guide for the development of state and local emergency operations plans, CPG 1–8*. Washington, DC: FEMA—Federal Emergency Management Agency.

FEMA—Federal Emergency Management Agency. (1998). *Principles of Emergency Management, Student Manual and Instructor Guide, G230*. Emmitsburg: FEMA Emergency Management Institute.

FEMA—Federal Emergency Management Agency. (2004). *National incident management system (NIMS): An introduction*. Washington, DC: FEMA—Federal Emergency Management Agency.

FEMA—Federal Emergency Management Agency. (2010). *Developing and maintaining emergency operations plans: Comprehensive preparedness guide (CPG) 101, version 2.0*. Washington, DC: FEMA—Federal Emergency Management Agency.

FEMA—Federal Emergency Management Agency. (2017). *National incident management system* (3rd ed.). Washington, DC: FEMA—Federal Emergency Management Agency.

Gillespie, D. F. (1991). Coordinating community resources. In T. E. Drabek & G. J. Hoetmer (Eds.), *Emergency management: Principles and practice for local government* (pp. 55–78). Washington, DC: International City Management Association.

Jensen, J., & Thompson, S. (2016). The incident command system: A literature review. *Disasters, 40*(1), 158–182.

Lindell, M. K. (2013). Disaster studies. *Current Sociology Review, 61*, 797–825.

Lindell, M. K. (2019). Chapter 1: An overview of hazards, vulnerability, and disasters. In M. K. Lindell (Ed.), *The Routledge handbook of urban disaster resilience: Integrating mitigation, preparedness, and recovery planning*. New York: Routledge.

Lindell, M. K., & Perry, R. W. (1980). Evaluation criteria for emergency response plans in radiological transportation. *Journal of Hazardous Materials, 3*, 335–348.

Lindell, M. K., & Perry, R. W. (1992). *Behavioral foundations of community emergency planning*. Washington DC: Hemisphere Press.

Lindell, M. K., Prater, C. S., & Perry, R. W. (2006). *Fundamentals of emergency management*. Emmitsburg: Federal Emergency Management Agency Emergency Management Institute. Available at www.training.fema.gov/hiedu/aemrc/booksdownload/fem/.

Lutz, L. D., & Lindell, M. K. (2008). Incident command system as a response model within emergency operation centers during Hurricane Rita. *Journal of Contingencies and Crisis Management, 16*(3), 122–134.

Noll, G. G., & Hildebrand, M. S. (2012). *Hazardous materials: Managing the incident* (4th ed.). Burlington: Jones & Bartlett Learning.

NRC—National Research Council. (2006a). *Terrorism and the chemical infrastructure: Protecting people and reducing vulnerabilities*. Washington, DC: NRC—National Research Council.

NRC—National Research Council. (2006b). *Facing hazards and disasters: Understanding Human Dimensions*. Washington DC: National Academy of Sciences/National Research Council.

NRT—National Response Team. (1987). *Hazardous materials emergency planning guide, NRT-1*. Washington, DC: NRT—National Response Team.

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review, 23*(1), 59–76.

Perry, R. W. (2018). Defining disaster: An evolving concept. In H. Rodríguez, J. Trainor, & W. Donner (Eds.), *Handbook of disaster research* (2nd ed., pp. 3–22). New York: Springer.

USNRC—US Nuclear Regulatory Commission/Federal Emergency Management Agency. (1980). *Criteria for preparation and evaluation of radiological emergency response plans and preparedness in support of nuclear power plants, NUREG-0654/FEMA-REP-1*. Washington DC: USNRC—US Nuclear Regulatory Commission/Federal Emergency Management Agency.

Wenger, D., Quarantelli, E. L., & Dynes, R. (1990). Is the incident command system a plan for all seasons and emergency situations? *Hazard Monthly, 10*(March), 8–12.

Emergency Management: Evacuations

Michael K. Lindell
Department of Urban Design and Planning, Institute for Hazards Mitigation Planning and Research, University of Washington, Seattle, WA, USA

Keywords

Risk area · Evacuation route system (ERS) · Evacuation demand · Evacuation capacity · Contraflow · Phased evacuation · Evacuation re-entry

Definition

Evacuation is a process intended to temporarily move people from a hazardous location to a place of greater safety.

Introduction

This entry addresses vehicular evacuation from environmental hazards, but not pedestrian evacuation from buildings, aircraft, or ships because the scale and dynamics of these evacuations is quite different (Aguirre et al. 2011; Bolton 2007; Nelson and Mowrer 2002; Peacock et al. 2011). Moreover, the focus is on preimpact rather than postimpact evacuations because preimpact evacuations face the challenge of clearing the risk area before the beginning of hazard exposure (Cova et al. 2017).

Small-scale evacuations can be improvised by risk area residents without any coordination by authorities, as was the case in the American Samoa tsunami (Lindell et al. 2015). Large-scale evacuations take place surprisingly frequently; an evacuation involving 1000 people or more takes place every 2–3 weeks in the United States (Dotson and Jones 2005). Moreover, evacuations are effective; many people are removed from the threats of natural hazards such as floods, hurricanes, wildfires, and volcanic eruptions and of technological hazards such as explosions, toxic chemical spills, and radiological releases. Despite its frequency and success, however, evacuation is not an unquestionably appropriate response to all environmental hazards. For example, many tornadoes, toxic chemical releases, and radiological incidents have such a rapid onset and short duration that sheltering in-place would be more appropriate. Evacuation would also be inadvisable for people whose risk of movement exceeds the risk of sheltering in-place, as could be the case for intensive care patients (see *Emergency management: Sheltering in-place*).

The logistics of evacuation are relatively simple when authorities can provide adequate forewarning of a localized hazard in areas where households have their own cars and have friends or relatives to stay with until it is safe to return home. However, the challenges of evacuation management increase substantially with the size of the risk area and its population. Although the risk area for a small daytime release of many toxic gases is only about 1/2 mile downwind (USDOT 2008), other hazards involve much larger areas. A nighttime spill of a large quantity of methyl isocyanate has a downwind protective action distance of 7 miles or more (USDOT 2008), and a nuclear power plant accident might require an evacuation of the entire 10 mile emergency planning zone (EPZ) (McKenna 2000).

Contrary to some people's beliefs, even large scale evacuations are quite safe; the accident rate for private vehicles is almost certain to be no higher and is quite likely to be lower than during normal driving periods (Lindell and Perry 1992). This is because traffic flow tends to be slow, moving at about 35 mph and unidirectional (outbound), so collisions are less severe and, therefore, less likely to produce deaths or injuries or to severely obstruct traffic flow. Moreover, the available evidence on hospital and nursing home evacuation indicates that even mass evacuations of special susceptibility populations can be accomplished in short time periods without appreciable safety risks. There are, of course, important logistical barriers that must be overcome in order to assure that an evacuation is carried out in a timely and effective manner (Chenault et al. 1980).

The remainder of this entry is divided into three major sections. The first section covers preimpact activities involved in evacuation planning. The second section summarizes Lindell, Murray-Tuite, Wolshon, and Baker's (2018) comprehensive discussion of evacuation analysis – the activities associated with assessing the time required to evacuate a risk area and the points on the evacuation route system (ERS) where bottlenecks are most likely to occur. The third section addresses evacuation management – the activities involved in actually implementing an evacuation plan.

Evacuation Planning

Disaster researchers (Lindell 2012; Lindell et al. 2006) and evacuation planners (Houston 2009) agree that a critical first step in evacuation planning is to establish continuing contact among all of the organizations that will be involved in implementing an evacuation – especially emergency management, transportation, police and fire departments, social services, and the American Red Cross (or other shelter operators). In the case of regional evacuations, this includes the

affected organizations in other jurisdictions – counties or states – that will be involved in evacuation, shelter, and re-entry. As will be discussed below, an effective planning process will establish as coordinated response to the issues that need to be addressed in risk, transit, and host jurisdictions.

In addition, emergency managers should recognize that evacuation management, like any other emergency response activity, generally requires *improvisation* as well as *planning* (Kreps 1991; Mendonça and Wallace 2004, 2007). Improvisation is usually needed because the incidents that occur do not correspond exactly to the scenarios that guided plan development. Consequently, it is essential that emergency exercises be conducted so responders learn how to adjust to conditions that they did not expect and that all incidents involving evacuations be thoroughly critiqued to ensure that lessons are learned, plans and procedures are revised, and training is adapted for a better response to future incidents (see the entry on ► "Emergency Management: Crisis Management and Response").

Evacuation Analysis

Evacuation analysis is one component of population protection analysis which, in turn, is one element in community preparedness analysis (Lindell and Perry 2007). There are five steps in evacuation analysis. These are to (a) identify risk areas/sectors, (b) assess the size of the risk area population, (c) identify the evacuation route system (ERS) and assess its capacity, (d) forecast evacuation demand, and (e) model traffic behavior.

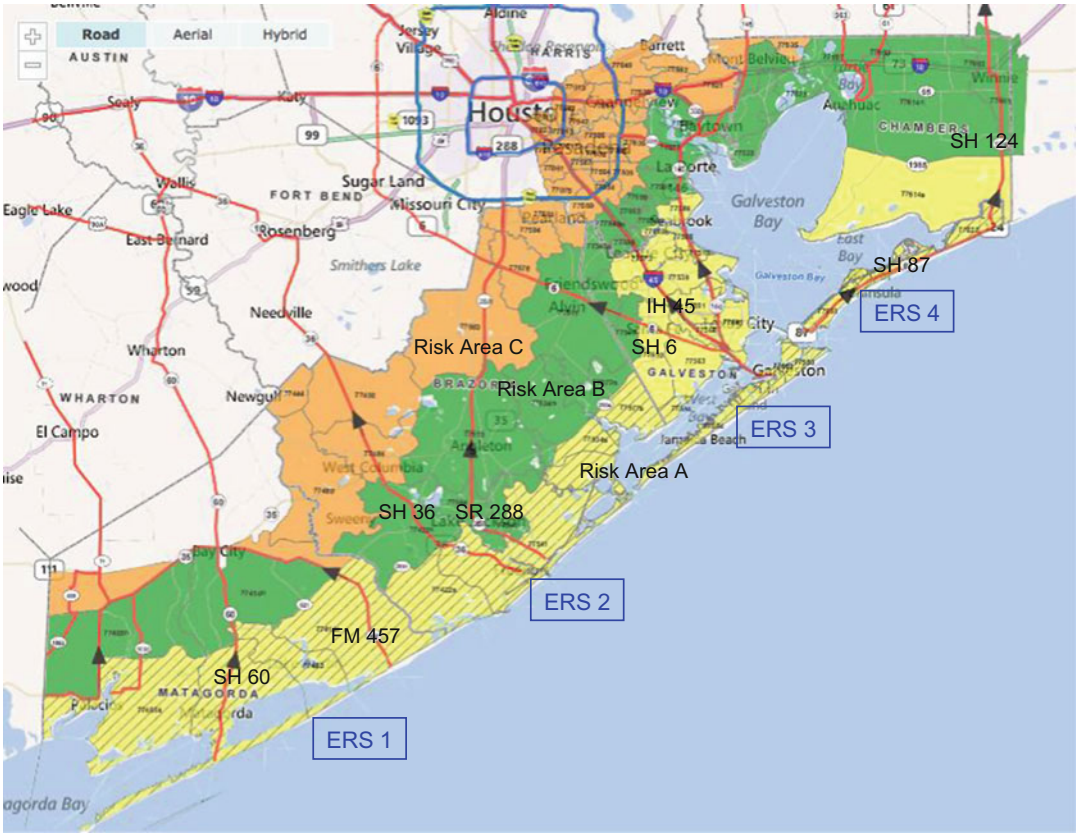
Identify Risk Areas/Sectors

A *risk area* comprises, as the name implies, the geographic areas at risk from a given hazard. For some hazards, equivalent terms are used such as a special flood hazard area (floods), vulnerable zone (VZ) (toxic chemicals), or EPZ (nuclear power plants). For most hydrometeorological and geological hazards, specialized agencies conduct risk analyses and provide risk area maps. However, identification of risk areas for hazardous materials is more difficult because the size of the risk area depends upon a number of factors, such as the quantity of material released, its volatility, toxicity (or radioactivity), and meteorological conditions such as wind speed, wind direction, and atmospheric stability. The USDOT (2008) provides simplified procedures for identifying risk areas for hazardous materials transportation, and the US Environmental Protection Agency (www.epa.gov/oem/tools.htm) provides procedures for fixed site facilities. There is a standardized 10-mile plume inhalation EPZ for all US commercial nuclear power plants (USNRC/FEMA 1980).

Whether for a natural (e.g., hurricane) or fixed-site technological (e.g., nuclear power plant) hazard, it is unlikely that all parts of an extremely large risk area will be advised to take the same protective action in an emergency. The most effective way to implement such protective actions is by identifying Emergency Response Planning Areas (ERPAs) – often called sectors in hurricane planning – that are areas of relatively homogeneous risk in which residents will all be advised to take the same protective action. Since these ERPAs or sectors should also be readily identifiable by those within them, emergency planners sometimes define them in terms of postal codes. This is necessary because many people have difficulty in identifying their location on risk area maps (Arlikatti et al. 2006; Zhang et al. 2004). Defining ERPAs by postal codes can work well in urban areas because postal codes in such areas are relatively compact (see Fig. 1). However, this can be problematic in rural areas if a single postal code covers a very large area having heterogeneous levels of risk. In such cases, ERPA boundaries can be defined by well-known political boundaries (city lines), geographical features (rivers), and major roads.

Assess the Size of the Risk Area Population

Vehicle-owning resident population. The basic unit of the vehicle-owning resident population is the household. The term *household* is important here because it is well documented that households tend to evacuate as a unit and will often seek to reunite if separated before evacuating (Tierney et al. 2001). The speed at which such households can evacuate thus depends on whether



Emergency Management: Evacuations, Fig. 1 Risk areas and the evacuation route system for the Houston/Galveston study area

members are united at the time of warning receipt, which is typical on evenings and weekends, and, if not, how soon they can reunite. However, there are times when households with multiple vehicles leave at different times after they have reunited (Maghelal et al. 2016). Moreover, depending upon the immediacy of the threat (usually minutes of forewarning for transportation accidents but days for hurricanes) and the potential for property destruction (low for toxic chemicals and high for hurricanes), people might take time to protect property (e.g., install storm shutters) or to pack valuables before evacuating. Most households have multiple members, which determines the required capacity of public shelters. In addition, most households have multiple vehicles and trailers, which increases the number of vehicles that need to be included in the estimates of evacuation demand.

Transit dependent population. The number of households without vehicles can be estimated by using data available from the National Household Travel Survey (nhts.ornl.gov/tools.shtml). Although the percentage of households without vehicles can be multiplied by the number of households in that area to estimate the number of households that will need public transit to evacuate, such estimates should be treated with caution. On one hand, some households have vehicles that are in poor repair and cannot provide reliable transportation over the long distances that are required for hurricane evacuations. On the other hand, some households that do not own vehicles are likely to obtain rides with other households that do. These two effects tend to cancel each other, but the relative magnitude of the two effects is unknown.

Transients. Transients can be individuals visiting the area on business or households

vacationing in the area. Transient populations can vary substantially by time of year, day of week (especially weekday vs. weekend), time of day, and also due to special events such as festivals and athletic events. Consequently, evacuation planners must be aware of this variation and incorporate it into their plans.

Special needs population. The special needs population comprises people with a variety of functional limitations in communication, medical health, functional independence, supervision, and transportation (FEMA 2010a, b; Kailes and Enders 2007). Some members of the special needs population are school children who must be evacuated directly to a safe location or who must be returned to their homes where they will evacuate with the other members of their households. Another important category of the special needs population is prisoners who must be evacuated under close supervision to another correctional institution – preferably before the rest of the risk area population begins to evacuate. A third major category in the special needs population comprises those who are institutionalized in hospitals, nursing homes, group homes, or other types of facilities (see Lindell et al. 2018, Table 3.3). Finally, 17% of the non-institutionalized US population has disabilities that substantially limit one or more of activities of daily living (Brault 2008). Thus, there is likely to be a significant fraction of the population in any risk area that will need some type of assistance when evacuating but whose location and specific needs are difficult to identify in advance. Mechanisms such as 2-1-1 calls are an important source of information for determining what types of vehicles will be needed and the types of facilities to which people with disabilities should be transported (Bame and Arlikatti 2019).

Time variation in ERPA population size. Evacuation analysts must recognize that the size of each population segment within each ERPA varies over time. There is variation by time of day as people travel to work, school, and other daytime activities and return home at night. This diurnal variation is most pronounced during the work week, but there can also be substantial variation by time of year in some communities, as tourists and people with second homes arrive in vacation communities. Finally, there can be substantial increases in population due to major festivals and sports events.

Identify the ERS and Its Capacity

Evacuations typically result in substantially more vehicles than normal attempting to use the ERS and, moreover, using those roads almost exclusively to travel in a single direction away from the hazard. Thus, continuing to use normal traffic control mechanisms such as stop signs and traffic signals – and even toll booths on tollways – can substantially delay vehicles attempting to reach safety. Consequently, it is necessary to designate the roads with the greatest capacity as the primary evacuation routes and to devise traffic management strategies that can be used to maximize their capacity.

The capacity of the ERS can be estimated in three steps. First, the analyst must identify the distinct set of links (individual road segments) that provide routes out of the risk area. Second, the analyst must assess the capacities of the individual links considering each link's number of lanes, shoulder type and width, intersection characteristics (including turn lanes and signal phasing), speed limits, and surrounding land use (Dotson and Jones 2005; TRB 2010). Third, the analyst must examine the configuration of the links in each evacuation route to determine whether they form a serial, parallel, converging, or diverging pattern. Serial links generally are limited by the smallest capacity in the set of links for that evacuation route – as when a link with an 800 vehicle per hour (vph) capacity overloads a link with a 600 vph capacity producing an overall capacity of 600 vph. It is also possible for the reverse to be true, as when a link with a 600 vph capacity underloads a link with an 800 vph capacity, also producing an overall capacity of 600 vph. However, there usually are additional vehicles attempting to access the downstream link, so a downstream link with greater capacity than the upstream link that feeds it usually becomes filled anyway.

In general, parallel links have additive capacities – as when two parallel links with capacities

of 800 vph have a combined capacity of 1600 vph. Diverging links (a single link splitting into multiple links generally follow the same rule as serial links because, here too, the capacity of the overall evacuation route is determined by the capacity of the link with the smaller capacity. Converging links (multiple links feeding into a single link) are problematic because traffic cannot merge seamlessly so the actual flow into the downstream route is likely to be lower than its nominal level.

It is important to recognize that link capacity can be degraded by both controllable and uncontrollable conditions. The controllable traffic impediments can usually be corrected (e.g., traffic accidents) or temporarily suspended (e.g., road repairs) to return traffic capacity to its normal level. The uncontrollable impediments (e.g., adverse weather) may require the use of compensatory actions such as additional evacuation routes or earlier evacuation initiation.

Estimate Evacuation Compliance and Shadow Evacuation

Evacuation managers should expect incomplete compliance with evacuation recommendations that is a function of authorities' labeling of the evacuation (recommended vs. mandatory) as well as people's perception of their distance from that threat (see Lindell and Prater 2007). However, they should also expect *shadow evacuation* – evacuation from areas that authorities do not consider to be at risk (Zeigler et al. 1981). Both incomplete compliance and shadow evacuation have been observed in both technological and natural hazards. In particular, evacuation shadow can reach surprisingly high levels. For example, the nuclear power plant accident at Three Mile Island produced about 150,000 evacuees in response to an evacuation advisory that applied to 10,000 people at most (Lindell and Perry 1983). Similarly, there was an estimated 47% evacuation rate from Harris County, Texas, for Hurricane Rita (Lindell and Prater 2008; Stein et al. 2010) even though less than 10% of the population was in the officially designated hurricane risk area.

Forecast Evacuation Demand

Following Urbanik et al. (1980), the time required for a household to evacuate after incident initiation can be defined as a function of four time components:

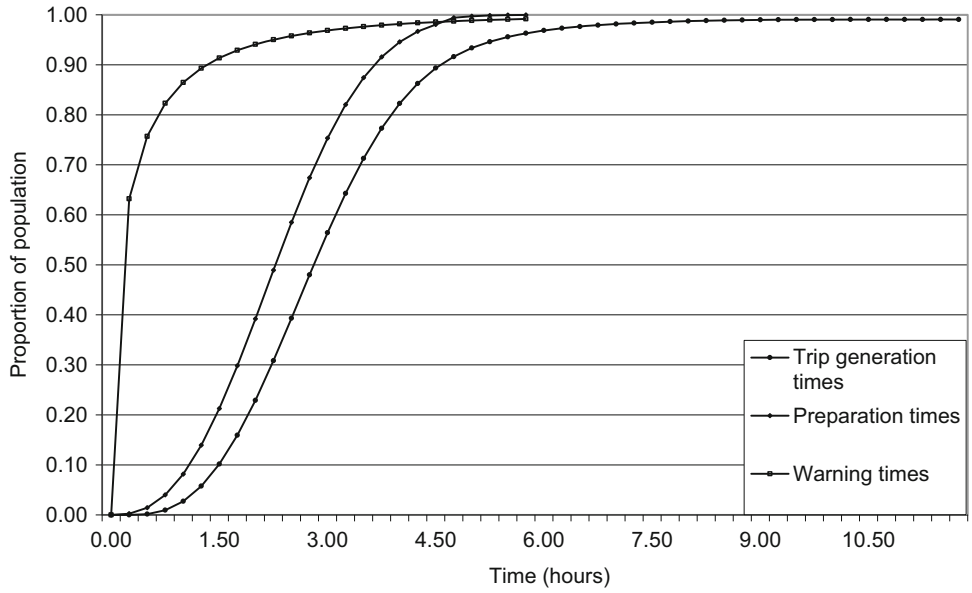
$$t_T = f\left(t_d, t_w, t_p, t_e\right) \quad (1)$$

where

- t_T is a household's total clearance time,
- t_d is the authorities' decision time,
- t_w is the household's warning receipt time,
- t_p is the household's evacuation preparation time, and
- t_e is the household's evacuation travel time.

Authorities' decision times (t_d) are critically important in rapid onset incidents for which there are no environmental cues, such as remote tsunamis and some toxic chemical releases. However, authorities' decisions can also be important in slow-onset incidents such as hurricanes because official protective action recommendations provide an indication of the time at which those at risk need to take protective action. The time to warning receipt (t_w) is highly variable because it depends on the nature of the local warning mechanisms. These warning mechanisms differ in many ways – with those having the lowest sender and receiver requirements (i.e., specialized equipment) having the slowest rate of dissemination (Lindell et al. 2018, Chap. 3). Household preparation time (t_p) is also highly variable because it depends on the amount of forewarning and people's threat perceptions. For example, people are likely to gather the family and leave immediately when they expect the imminent arrival of a toxic chemical release.

The first three components in Eq. 1 (t_d, t_w, and t_p) are combined to produce an estimate of the cumulative percentage of departing vehicles at each point in time (see Fig. 2). The resulting departure time distribution – the "loading function" – is multiplied by the number of evacuating vehicles to estimate evacuation demand – the rate at which vehicles enter the ERS. The rate of warning reception and evacuation preparation can each be represented as an exponential function,



Source: Lindell (2008)

Emergency Management: Evacuations, Fig. 2 Generic trip generation time distribution function. (Source: Lindell 2008)

$p_t = 1 - \exp(-at^b)$, where p_t is the proportion of the population prepared at time t, and a and b are parameters that determine the shape of the curve. For example, Lindell (2008) reported an analysis that used parameters $a = 2.00$, $b = 0.50$ for a representative warning time distribution and $a = 0.085$, $b = 2.55$ for a representative scenario preparation time distribution. These distributions would be appropriate for a rapid onset scenario such as a flash flood or hazardous materials release. However, they are inappropriate for hurricane evacuations in major metropolitan areas where evacuations take place over two or more days. In such cases, the departure time distributions *for each day* tend to have departure rates (per hour) that rise from 6 am to 6 pm, decline in the afternoon and evening, and drop to nearly zero overnight (Lindell et al. 2018, Chap. 5).

It is important to note that the shape of the warning distribution depends upon the nature of the warning system (Rogers and Sorensen 1988; Sorensen and Rogers 1989). The larger the percentage of the population that can be warned *simultaneously by broadcast systems* (e.g., siren and Emergency Alert System), the sooner the warning distribution will reach asymptote (the point at which everyone who can receive a warning does so). Conversely, the larger the percentage of the population that must be warned *sequentially by diffusion systems* (e.g., emergency responders going door-to-door), the later the warning distribution will reach asymptote. By contrast, the shape of the preparation time distribution depends upon warning recipients' perceptions of the urgency of the situation and their abilities to respond promptly. For example, people will begin their evacuations sooner for a chemical release in progress than for a hurricane that is 2 days away. In addition, able-bodied people whose families are united and who have emergency kits already packed will begin their evacuations sooner than those who lack these characteristics. In incidents with long forewarning periods, preparation time distributions cannot only consist of preparation to leave work, travel from work to home, and activities to prepare for the evacuation trip, but also intermediate trips to get money, and to purchase gas, food, and medicine.

The estimation of the ERS loading function is even more complex for situations in which there is no forewarning before hazard onset – *no-notice*

evacuations. In such cases, families are likely to be separated with, for example, two spouses working at different locations and multiple children at different schools. Families' attempts to reunify constitute an additional component of preparation time (before beginning their trip out of the risk area) that can produce inbound traffic into the risk area and cross-flows through the risk area. This delays households' own departures and disrupts outbound flows of traffic from those seeking to leave directly after receiving a warning (Murray-Tuite 2007; Murray-Tuite and Mahmassani 2003, 2004).

Model Traffic Behavior

Finally, household evacuation travel time (t_e) varies depending on the capacity of the ERS and the demand for space on that ERS. This time component is estimated using one of the available traffic optimization or simulation codes (see Lindell et al. 2018, Chap. 9). In a very simple case, the time required to evacuate a risk area could be estimated by dividing the number of evacuating vehicles by the roadway capacity (in vehicles per hour). Unfortunately, evacuations frequently produce demand that exceeds the available roadway capacity, thus producing queues of vehicles waiting for access to the roadway. The need to incorporate queuing time into the calculations means that modeling traffic behavior for any area other than a small neighborhood with an extensive road network requires complex computations. Only computer programs can adequately model the behavior of drivers as they leave their points of origin, drive to one of the principal evacuation routes, queue for access to the evacuation route, travel along that route to a proximal destination at the edge of the risk area, and travel from there to the household's ultimate destination where they will seek shelter. These models require analysts to input the data from the previous stages of the evacuation analysis – identifying risk areas/sectors, assessing the size of the risk area population, identifying the ERS and its capacity, and forecasting evacuation demand. These traffic modeling programs can generate data on total traffic volume; average vehicle travel time; risk area clearance time; hourly volume, total volume, and average speed at each exit from the risk area; and queue lengths at selected intersections (Jones et al. 2011). It is important to conduct sensitivity analyses using a range of plausible values for each of the major input parameters to see how model output data, especially evacuation time estimates, are affected (Lindell 2008).

Evacuation Management

The principal tasks involved in managing an evacuation are threat detection and emergency classification, protective action selection, population warning, evacuation transportation support, evacuation traffic management, reception and care (shelter accommodations), and re-entry management (Lindell et al. 2006). There are other response functions that must be performed in an emergency, but they are not directly related to evacuation management (see *Emergency management: Crisis management and response*).

Threat Detection and Emergency Classification

Sometimes, as was the case in the 1978 Sumner Washington flood, the risk area population needs no assistance in detecting and classifying environmental conditions as immediately dangerous (Perry et al. 1981). In other cases, such as hurricanes and nuclear power plant accidents, specialized agencies are needed to detect a hazard, forecast the areas it is likely to affect, and assess the severity of the threat to people and property – thus indicating the need for sheltering in-place or evacuation. For example, the National Weather Service uses two emergency classes, *Watch* and *Warning*, to define the certainty, severity, immediacy, and intensity of the threat at designated locations. Once the agency (or facility in the case of nuclear power plants and chemical facilities) detects and classifies the threat, it needs to notify local emergency managers so they can decide whether to initiate protective actions such as evacuation. However, Sorensen and Rogers (1988) found that few communities had adequate mechanisms for receiving notifications about incidents from chemical facilities within their

jurisdiction and other studies have found delays in receiving and acting on such threat notifications (Lindell et al. 2017; Sorensen and Mileti 2016).

Protective Action Selection

It is important to recognize that evacuation is unnecessary – and might be dangerous – for those who can achieve protection by sheltering in-place (Cova et al. 2009; Jetter and Whitfield 2005; Lindell and Perry 1992; Sorensen et al. 2004). Sheltering in-place within buildings is effective when these structures are elevated above the flood crest, are strong enough to withstand hurricane wind, can withstand wildfires, are dense enough to provide shielding from external radiation, or have sufficiently low air exchange rates that they delay the infiltration of contaminated air (*Emergency management: Sheltering in-place*). In addition to deciding which protective actions to recommend, local authorities need to decide when to initiate those protective actions. That is, "who should be warned to do what and when?" (Cova et al. 2017; Lindell et al. 2018, Chap. 3).

Population Warning

Warnings are crucial elements in initiating evacuation, but emergency managers need to understand the best ways to construct and transmit them (see Lindell 2018; Lindell and Perry 2004). First, a warning message should indicate the warning source, describe the threat in terms of its expected impact intensity, timing, and location, provide a recommended protective action, and indicate sources to contact for further information about the situation and to obtain assistance in taking protective action. Warnings should be transmitted repeatedly on each channel and disseminated via multiple channels so people receive, attend to, and understand the warning message.

There are many different channels for disseminating warnings to those at risk (*Emergency management: Emergency alert systems*). These are face-to-face warnings, mobile loudspeakers, sirens, commercial radio and television, NOAA Weather Radio, telephones, email, Internet websites, social media such as Twitter, and newspapers. Each of these mechanisms can be evaluated with respect to eight characteristics. These are precision of dissemination (the ability to target only those at risk), penetration of normal activities (especially the ability to overcome ambient noise), specificity of the message (the ability to convey all of the elements of an ideal warning message), susceptibility to message distortion (a problem that arises when a warning message must be passed through one or more intermediate communicators), rate of dissemination over time (the time between receipt by the first and last warning receivers), receiver requirements (especially expensive equipment or specialized knowledge and skill), sender requirements (also expensive equipment or specialized knowledge and skill), and feedback (sender verification that the receiver has received the warning). Communities need to choose which warning channels they will use based upon the characteristics of the hazard (especially the amount of forewarning, the size of the impact area, and the likely impact intensity) and the community's financial resources (Lindell et al. 2018, Chap. 3).

Evacuation Transportation Support

As noted earlier, some segments of the risk area population lack vehicles or have other obstacles to evacuation. For the transit dependent, local authorities need to make arrangements with school districts or mass transit providers such as transit districts. Emergency managers need to verify that transit providers have not made arrangements with other jurisdictions that would need buses at the same time. Such duplicate demands could arise if the providers signed agreements with officials in two different counties on the assumption that these agreements would be activated only for very local evacuations that would not require simultaneous evacuations in multiple jurisdictions (Daines 1991). Similar caution must be taken to review concurrent service agreements for multiple hospitals and nursing homes, which have the added requirement of ensuring that there are available beds in receiving facilities before transporting patients (Auf der Heide and Scanlon 2007). Moreover, care must be taken to ensure that the number of buses, ambulances, and other

vehicles is sufficient to accommodate the maximum capacity of these facilities. Criteria for transporting pets need to be made and publicized via the news media before and during an incident (Heath et al. 2001).

Evacuation Traffic Management

There are two fundamental strategies for evacuation traffic management: ERS capacity management and evacuation demand management. ERS capacity management seeks to minimize or avoid queues that form when too many vehicles compete for space on the roads or to increase capacity through procedures such as contraflow. Evacuation demand management seeks to regulate the number of vehicles attempting to use the ERS at any given point in time so that maximum capacity is maintained for a given lane use configuration.

ERS capacity management. The most common evacuation impediments are ERS capacity and ERS condition (Vásconez and Kehrli 2010). Accordingly, maintaining – and if possible increasing – ERS capacity is a major issue in managing an evacuation. The primary methods for maintaining ERS capacity are intersection control and prompt clearance of traffic impediments such as vehicles blocking traffic lanes due to overheating, running out of fuel, and collisions (Ballard and Borchardt 2006; Jones et al. 2011; Wolshon et al. 2005). Some traffic impediments can be avoided by, for example, stationing fuel tankers along evacuation routes to avoid allowing evacuating vehicles to run out of fuel. Some collisions can be cleared by other evacuating vehicles that push the incapacitated vehicle off the roadway, but others require authorities to station tow trucks along the evacuation routes.

The primary methods for increasing ERS capacity are utilization of highway shoulders as *evaculanes,* crossing elimination, special signal timing, and implementation of contraflow – reversing the direction of inbound lanes (Jones et al. 2011; Wolshon et al. 2005). Utilizing shoulders as traffic lanes has some distinct limitations such as precluding their use for emergency vehicle access to accident sites (Ballard and Borchardt 2006). Moreover, they also only increase capacity by a small amount (estimated to be 8%, Wolshon et al. 2005). However, the cumulative effect of even this small capacity increase could be significant if implemented over multiple evacuation routes.

Special signal timing limits the amount of time allocated to crossing and turning maneuvers at intersections on designated evacuation routes, whereas crossing elimination prevents them altogether. In both cases, the objective is to maximize the flow of traffic on the outbound route away from the hazard zone. Contraflow reverses the direction of one or more travel lanes from inbound (toward the hazard zone) to outbound. Planning for contraflow requires careful planning because a full contraflow configuration provides more outbound capacity, but partial contraflow configurations (reversing only one of two inbound lanes) provide an opportunity to maintain one or more lanes in their normal inbound configuration for returning buses and emergency vehicles. This obviously increases outbound capacity by a smaller amount (about 30%) than a complete contraflow configuration (about 70%) and also increases the potential for head-on collisions. Regardless of which contraflow configuration is selected, evacuation managers need to correctly anticipate the length of time required to implement it, which range from 4 to 12 h, depending on the length and complexity of the contraflow segment (Wolshon et al. 2005).

Evacuation demand management. The primary methods of demand management are to control the total number of people seeking to use the evacuation routes, control the allocation of vehicles to evacuation routes, and control the loading of the ERS. One important method of demand management is to avoid shadow evacuation from outside the officially designated evacuation zones. As noted earlier, shadow evacuation has added substantially to the number of vehicles in some past evacuations. In addition, evacuation managers can reduce the amount of background traffic, which consists of vehicles attempting to use the evacuation routes for routine travel, by controlling access to the evacuation zone. The need for evacuation from inside the risk area can also be reduced if local structures are adequate for sheltering in-place. Moreover, the occupants must

believe that these structures provide effective protection before they will comply with a shelter in-place recommendation.

Another demand management strategy is to reroute evacuation traffic from overutilized routes to underutilized ones. This could be an effective strategy because people tend to use the most familiar routes to their evacuation destinations (Lindell and Prater 2007). Unfortunately, such habits tend to overload freeways and underload minor highways (Dow and Cutter 2002). The challenge in redirecting traffic is for authorities to identify the alternative evacuation routes from specific originating points to specific destinations and to communicate in real time what are average speeds on these routes. This strategy is increasingly feasible with the development of intelligent transportation systems that are capable of monitoring and directing traffic.

In principle, ERS loading can be controlled by phased (also called "staged") evacuations in which people in areas of lower risk are asked to delay their evacuations until after people in areas of higher risk have evacuated (Jones et al. 2007, 2011). Phased evacuations have been used many times in hurricanes and wildfires (Jones et al. 2008). However, conclusions about their utility appear to be based only on anecdotal evidence of success (i.e., an absence of spectacular failures) rather than collection and analysis of empirical data. To implement phased evacuation effectively, evacuation managers need high levels of evacuee compliance with the phased evacuation recommendation and an ability to forecast accurately how soon people would begin to evacuate after a delayed evacuation advisory is issued. Unfortunately, there is no research on the amount of time people are willing to delay their evacuations while others are leaving. To the contrary, the available behavioral research indicates that people believe that sheltering in-place provides less effective protection than evacuation for toxic chemical releases (Lindell and Perry 1992). Experts are also highly uncertain about people's willingness to comply with a shelter in-place recommendation in a radiological release (Dombroski et al. 2006), and observation of others evacuating is a social cue that prompts people to leave (Huang et al. 2016). Notwithstanding these uncertainties, there is a natural tendency for those farther inland to begin their hurricane evacuations later than those near the coast (Lindell et al. 2011; Wu et al. 2012). This has the potential to create traffic jams if inland residents try to enter the ERS as the same time coastal residents are arriving there. Fortunately, this convergence of coastal and inland evacuees has the tendency to produce evacuation queues in inland areas where the risk of being overtaken by the hurricane surge is relatively low.

Reception and Care

When evacuations last overnight or longer, people need places to stay until it is safe to return home. The types of accommodations people choose is well studied, with researchers finding consistently that only a small percentage of evacuees use public shelters. The Mileti et al. (1992) review concluded that only 15% of evacuees go to public shelters, which are primarily occupied by ethnic minorities, the poor, and those who depart too late to find hotel/motel vacancies. The Lindell et al. (2018, Chap. 6) review of hurricane evacuation studies found that 62% of evacuees stayed in peers' homes (range 54–70%), whereas 27% stayed in hotels/motels (range 16–32%), and only 3% stayed in public shelters (range 2–6%). That estimate of hurricane shelter usage is significantly lower than Mileti and his colleagues' (1992) estimate for evacuations in general – probably because hurricanes provide so much forewarning that people have an adequate amount of time to make arrangements for accommodations with peers or commercial facilities.

Re-entry Management

Managing evacuees' re-entry after an evacuation can be a major challenge for emergency managers. Achieving high levels of compliance with official re-entry plans has been difficult following past hurricanes (Siebeneck and Cova 2008), so there is a need to better understand the factors that influence the timing of evacuees' re-entry attempts. Siebeneck et al. (2013) found that Hurricane Ike evacuees who complied with official

re-entry plans expected greater problems being stuck in traffic and expected less physical risk from damaged structures. There were no statistically significant relationships of re-entry plan compliance with expectations of looting, income loss, utility loss, and socio-demographic characteristics.

Because many evacuees rely on news media as a source of information about their communities while evacuated (Siebeneck and Cova 2008), it is important to gain a better understanding of what information – or misinformation – the news media are communicating and how this, in turn, shapes the expectations and behavior of the evacuated population. Lin et al. (2014) found significant changes in the utilization of different sources of emergency information over the course of the Hurricane Ike evacuation, but local news media remained the most common sources throughout the event. There also were significant differences in the relative importance of different sources of reentry information, with people relying most on information from peers. Nonetheless, none of the information sources produced greater compliance with official reentry plans.

Conclusions

Evacuations can be managed effectively, but the larger the scale of the evacuation and the shorter the amount of forewarning, the greater is the need to plan, analyze, and manage effectively. Effective planning requires coordination among diverse agencies at different levels of government (municipal, county, state, and federal), as well as with nongovernmental organizations such as the Red Cross. Effective analysis requires identifying risk areas/sectors, assessing the size of the risk area population, identifying the ERS and its capacity, forecasting evacuation demand, and modeling traffic behavior. Effective evacuation management requires incident detection and classification, protective action selection, warning, evacuation transportation support, evacuation traffic management, shelter accommodations, and re-entry management. Evacuation managers have the best chance of protecting the risk area population from environmental hazards if they address all of these issues successfully. In addition, they should work with local emergency managers to increase households' and businesses' levels of emergency preparedness (Lindell 2013; Lindell and Perry 2007; Perry and Lindell 2007). Finally, historical evidence indicates that sound traffic management (for the evacuation of the general public by automobile) and a normal level of medical precaution (for hospital evacuations) are sufficient to assure the safety of the evacuating population.

Cross-References

- ▶ Emergency Management: Crisis Communication
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Preparedness and Planning
- ▶ Emergency Management: Shelter In-Place

Acknowledgments This research was supported by the National Science Foundation under Grants IIS-1540469, CMMI-1760766, and CMMI-1826455. None of the conclusions expressed here necessarily reflects views other than those of the author.

References

Aguirre, B. E., El-Tawil, S., Best, E., Gill, K. B., & Fedorov, V. (2011). Contributions of social science to agent-based models of building evacuation. *Contemporary Social Science, 6*, 415–432.

Arlikatti, S., Lindell, M. K., Prater, C. S., & Zhang, Y. (2006). Risk area accuracy and hurricane evacuation expectations of coastal residents. *Environment and Behavior, 38*, 226–247.

Auf der Heide, E., & Scanlon, J. (2007). The role of the health sector in planning and response. In K. J. Tierney & W. F. Waugh Jr. (Eds.), *Emergency management: Principles and practice for local government* (2nd ed., pp. 183–206). Washington DC: International City/County Management Association.

Ballard, A. J., & Borchardt, D. W. (2006). *Recommended practices for hurricane evacuation traffic operations*, FHWA/TX-06/0–4962-P2. College Station: Texas Transportation Institute. Downloaded from tti.tamu.edu.documents/0-4962.P2.psf

Bame, S. I., & Arlikatti, S. (2019). Unmet needs and community service planning for disasters. In M. K. Lindell (Ed.), *Disaster resilience: Integrating mitigation, preparedness, and recovery planning*. New York: Routledge.

Bolton, P. A. (2007). *Managing pedestrians during evacuation of metropolitan areas,* FHWA-HOP-07-066. Washington, DC: Federal Highway Administration. Downloaded from www.its.dot.gov/its_publicsafety/evacuation.htm

Brault, M. (2008). *Disability status and the characteristics of people in group quarters: A brief analysis of disability prevalence among the civilian noninstitutionalized and total populations in the American Community Survey.* Washington, DC: U.S. Census Bureau. Downloaded from www.census.gov/hhes/www/disability/GQdisability.pdf

Chenault, W. W., Hilbert, G. D., & Reichlin, S. D. (1980). *Evacuation planning in the TMI accident*. Mclean: Human Sciences Research. Downloaded from https://apps.dtic.mil/docs/citations/ADA080104

Cova, T. J., Drews, F. A., Siebeneck, L. K., & Musters, A. (2009). Protective actions in wildfires: Evacuate or shelter-in-place? *Natural Hazards Review, 10*, 151–162.

Cova, T. J., Dennison, P. E., Li, D., Drews, F. A., Siebeneck, L. K., & Lindell, M. K. (2017). Warning triggers in environmental hazards: Who should be warned to do what and when? *Risk Analysis, 37*, 601–611.

Daines, G. E. (1991). Planning, training, and exercising. In T. E. Drabek & G. J. Hoetmer (Eds.), *Emergency management: Principles and practice for local government* (pp. 161–200). Washington, DC: International City Management Association.

Dombroski, M., Fischhoff, B., & Fischbeck, P. (2006). Predicting emergency evacuation and sheltering behavior: A structured analytical approach. *Risk Analysis, 26*, 1675–1688.

Dotson, L. J., & Jones, J. (2005). *Identification and analysis of factors affecting emergency evacuations: Main report.* NUREG/CR-6864, Vol. 1, SAND2004–5901. Washington DC: US Nuclear Regulatory Commission.

Dow, K., & Cutter, S. L. (2002). Emerging hurricane evacuation issues: Hurricane Floyd and South Carolina. *Natural Hazards Review, 3*, 12–18.

FEMA—Federal Emergency Management Agency (2010a). *Developing and maintaining emergency operations plans: Comprehensive preparedness guide 101, Version 2.0*. Retrieved April 2012, from http://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf

FEMA—Federal Emergency Management Association (2010b). *Guidance on planning for integration of functional needs support services in general population shelters*. Retrieved April 2012, from http://www.fema.gov/pdf/about/odic/fnss_guidance.pdf

Heath, S. E., Kass, P. H., Beck, A. M., & Glickman, L. T. (2001). Human and pet-related risk factors for household evacuation failure during a natural disaster. *American Journal of Epidemiology, 153*, 659–665.

Houston, N. (2009). *Good practices in transportation evacuation preparedness and response: Results of the FHWA workshop series*, FHWA-HOP-09-040. Washington DC: Federal Highway Administration, Office of Transportation Operations. Downloaded from www.ops.fhwa.dot.gov/publications/publications.htm#eto

Huang, S.-K., Lindell, M. K., & Prater, C. S. (2016). Who leaves and who stays? A review and statistical meta-analysis of hurricane evacuation studies. *Environment and Behavior, 48*, 991–1029.

Jetter, J. J., & Whitfield, C. (2005). Effectiveness of expedient sheltering in place in a residence. *Journal of Hazardous Materials, A119*, 31–40.

Jones, J. A., Bixler, N., Schelling, F. J., & Sullivan, R. (2007). *Review of NUREG-0654, Supplement 3, "Criteria for protective action recommendations for severe accidents"*, NUREG/CR-6953, Vol. I, SAND2007-5448P. Washington DC: U.S. Nuclear Regulatory Commission. Downloaded from www.nrc.gov/reading-rm/doc-collections/nuregs/

Jones, J., Walton, F., Smith, J. D., & Wolshon, B. (2008). *Assessment of emergency response planning and implementation for large scale evacuations*, NUREG/CR-6981, SAND2008-1776P. Washington DC: US Nuclear Regulatory Commission. Downloaded from www.nrc.gov/reading-rm/doc-collections/nuregs/

Jones, J., Walton, F., & Wolshon, B. (2011). *Criteria for development of evacuation time estimate studies*, NUREG/CR-7002 SAND2010-0016P. Washington DC: US Nuclear Regulatory Commission. Downloaded from www.nrc.gov/reading-rm/doc-collections/nuregs/

Kailes, J. I., & Enders, A. (2007). Moving beyond "special needs". A function based framework for emergency management and planning. *Journal of Disability Policy Studies, 17*, 230–237.

Kreps, G. A. (1991). Organizing for emergency management. In T. S. Drabek & G. J. Hoetmer (Eds.), *Emergency management: Principles and practice for local government* (pp. 30–54). Washington, DC: International City/County Management Association.

Lin, C.-C., Siebeneck, L. K., Lindell, M. K., Prater, C. S., Wu, H. C., & Huang, S. K. (2014). Evacuees' information sources and reentry decision making in the aftermath of Hurricane Ike. *Natural Hazards, 70*, 865–882.

Lindell, M. K. (2008). EMBLEM2: An empirically based large-scale evacuation time estimate model. *Transportation Research, A, 42*, 140–154.

Lindell, M. K. (2012). Response to environmental disasters. In S. Clayton (Ed.), *Handbook of environmental and conservation psychology* (pp. 391–413). New York: Oxford University Press.

Lindell, M. K. (2013). Disaster studies. *Current Sociology Review, 61*, 797–825.

Lindell, M. K. (2018). Communicating imminent risk. In H. Rodríguez, J. Trainor, & W. Donner (Eds.),

Handbook of disaster research (pp. 449–477). New York: Springer.

Lindell, M. K., Murray-Tuite, P., Wolshon, B., & Baker, E. J. (2018). *Large-scale evacuation: The analysis, modeling, and management of emergency relocation from hazardous areas*. New York: Routledge.

Lindell, M. K., & Perry, R. W. (1983). Nuclear power plant emergency warning: How would the public respond? *Nuclear News, 26*, 49–53.

Lindell, M. K., & Perry, R. W. (1992). *Behavioral foundations of community emergency planning*. Washington, DC: Hemisphere Press.

Lindell, M. K., & Perry, R. W. (2004). *Communicating environmental risk in multiethnic communities*. Thousand Oaks: Sage.

Lindell, M. K., & Perry, R. W. (2007). Planning and preparedness. In K. J. Tierney & W. F. Waugh Jr. (Eds.), *Emergency management: Principles and practice for local government* (2nd ed., pp. 113–141). Washington, DC: International City/County Management Association.

Lindell, M. K., & Prater, C. S. (2007). Critical behavioral assumptions in evacuation analysis for private vehicles: Examples from hurricane research and planning. *Journal of Urban Planning and Development, 133*, 18–29.

Lindell, M. K., & Prater, C. S. (2008). *Behavioral analysis: Texas hurricane evacuation study*. College Station: Texas A&M University Hazard Reduction and Recovery Center.

Lindell, M. K., Prater, C. S., & Perry, R. W. (2006). *Fundamentals of emergency management*. Emmitsburg: Federal Emergency Management Agency Emergency Management Institute. Available at www.training.fema.gov/EMIWeb/edu/fem.asp or archone.tamu.edu/hrrc/Publications/books/index.html.

Lindell, M. K., Kang, J. E., & Prater, C. S. (2011). The logistics of household hurricane evacuation. *Natural Hazards, 58*, 1093–1109.

Lindell, M. K., Prater, C. S., Gregg, C. E., Apatu, E., Huang, S.-K., & Wu, H.-C. (2015). Households' immediate responses to the 2009 Samoa earthquake and tsunami. *International Journal of Disaster Risk Reduction, 12*, 328–340.

Lindell, M. K., Sorensen, J. H., & Baker, E. J. (2017). *Community response to hurricane threat: Estimates of temporal distributions of warning issuance, warning diffusion, and household mobilization (Draft)*. Davis: US Army Corps of Engineers Risk Management Center.

Maghelal, P., Peacock, W. G., & Li, X. (2016). Evacuating together or separately: Factors influencing split evacuations prior to Hurricane Rita. *Natural Hazards Review*. https://doi.org/10.1061/(ASCE)NH.1527-6996.0000226.

McKenna, T. (2000). Protective action recommendations based upon plant conditions. *Journal of Hazardous Materials, 75*, 145–164.

Mendonça, D., & Wallace, W. A. (2004). Studying organizationally-situated improvisation in response to extreme events. *International Journal of Mass Emergencies and Disasters, 22*, 5–29.

Mendonça, D., & Wallace, W. A. (2007). A cognitive model of improvisation in emergency management. *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans, 37*, 547–561.

Mileti, D. S., Sorensen, J. H., & O'Brien, P. W. (1992). Toward an explanation of mass care shelter use in evacuations. *International Journal of Mass Emergencies and Disasters, 10*, 25–42.

Murray-Tuite, P. (2007). Perspectives for network management in response to unplanned disruptions. *Journal of Urban Planning and Development, 133*, 9–17.

Murray-Tuite, P. M., & Mahmassani, H. S. (2003). Model of household trip-chain sequencing in emergency evacuation. *Transportation Research Record, 1831*, 21–29.

Murray-Tuite, P. M., & Mahmassani, H. S. (2004). Transportation network evacuation planning with household activity interactions. *Transportation Research Record, 1894*, 150–159.

Nelson, H. E., & Mowrer, F. W. (2002). Chapter 14, Emergency movement. In P. J. DiNenno et al. (Eds.), *SFPE handbook of fire protection engineering*. Quincy/Boston: National Fire Protection Association.

Peacock, R. D., Kuligowski, E. D., & Averill, J. D. (2011). *Pedestrian and evacuation dynamics*. New York: Springer.

Perry, R. W., & Lindell, M. K. (2007). *Emergency planning*. Hoboken: Wiley.

Perry, R. W., Lindell, M. K., & Greene, M. R. (1981). *Evacuation planning in emergency management*. Lexington: Heath Lexington Books.

Rogers, G. O., & Sorensen, J. H. (1988). Diffusion of emergency warnings. *Environmental Professional, 10*, 185–198.

Siebeneck, L. K., & Cova, T. J. (2008). An assessment of the reentry process for Hurricane Rita 2005. *International Journal of Mass Emergencies and Disasters, 26*, 91–111.

Siebeneck, L. K., Lindell, M. K., Prater, C. S., Wu, H. C., & Huang, S. K. (2013). Evacuees' reentry concerns and experiences in the aftermath of Hurricane Ike. *Natural Hazards, 65*, 2267–2286.

Sorensen, J. H., & Mileti, D. M. (2016). *First alert and/or warning issuance delay time estimation for dam breaches, controlled dam releases, and levee breaches and overtopping*. Davis: USACE Institute for Water Resources Risk Management Center.

Sorensen, J. H., & Rogers, G. O. (1988). Local preparedness for chemical accidents: A survey of U.S. communities. *Industrial Crisis Quarterly, 2*, 89–108.

Sorensen, J. H., & Rogers, G. O. (1989). Warning and response in two hazardous materials transportation accidents in the U.S. *Journal of Hazardous Materials, 22*, 57–74.

Sorensen, J. H., Shumpert, B. L., & Vogt, B. M. (2004). Planning for protective action decision making:

evacuate or shelter-in-place. *Journal of Hazardous Materials, A109*, 1–11.
Stein, R. M., Dueñas-Osorio, L., & Subramanian, D. (2010). Who evacuates when hurricanes approach? The role of risk, information, and location. *Social Science Quarterly, 91*, 816–834.
Tierney, K. J., Lindell, M. K., & Perry, R. W. (2001). *Facing the unexpected: Disaster preparedness and response in the United States*. Washington, DC: Joseph Henry Press.
TRB—Transportation Research Board. (2010). *Highway capacity manual*. Washington, DC: Author.
Urbanik, T., Desrosiers, A., Lindell, M. K., & Schuller, C. R. (1980). *An analysis of techniques for estimating evacuation times for emergency planning zones*, NUREG/CR-1745. Washington, DC: US Nuclear Regulatory Commission.
USDOT—US Department of Transportation (2008). *North American emergency response guidebook*. Retrieved May 29, 2012, from phmsa.dot.gov/hazmat/library/erg
USNRC/FEMA—US Nuclear Regulatory Commission/Federal Emergency Management Agency (1980). *Criteria for preparation and evaluation of radiological emergency response plans and preparedness in support of nuclear power plants*, NUREG-0654/FEMA-REP-1. Retrieved May 29, 2012, from www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0654/
Vásconez, K. C., & Kehrli, M. (2010). *Highway evacuations in selected metropolitan regions: Assessment of impediments*. FHWA-HOP-10-059. Washington DC: Federal Highway Administration, Office of Transportation Operations. Downloaded from www.ops.fhwa.dot.gov/publications/publications.htm#eto
Wolshon, B., Urbina Hamilton, E., Levitan, M., & Wilmot, C. (2005). Review of policies and practices for hurricane evacuation. II: Traffic operations, management, and control. *Natural Hazards Review, 6*, 143–161.
Wu, H. C., Lindell, M. K., & Prater, C. S. (2012). Logistics of hurricane evacuation in Hurricanes Katrina and Rita. *Transportation Research Part F: Traffic Psychology and Behaviour, 15*, 445–461.
Zeigler, D., Brunn, S., & Johnson, J. (1981). Evacuation from a nuclear technological disaster. *Geographical Review, 71*, 1–16.
Zhang, Y., Prater, C. S., & Lindell, M. K. (2004). Risk area accuracy and evacuation from Hurricane Bret. *Natural Hazards Review, 5*, 115–120.

Further Reading

Lindell, M. K., Murray-Tuite, P., Wolshon, B., & Baker, E. J. (2019). *Large-scale evacuation: The analysis, modeling, and management of emergency relocation from hazardous areas*. New York: Routledge.
Tierney, K. J., & Waugh, W. F., Jr. (Eds.). (2007). *Emergency management: Principles and practice for local government* (2nd ed.). Washington, DC: International City/County Management Association.

Emergency Management: Incident Command System

Dorothy Moses Schulz
Law, Police Science, and Criminal Justice Administration, John Jay College of Criminal Justice (CUNY), New York, NY, USA

Keywords
Risk · Vulnerability · Disaster management

Definition

Emergency management describes the activities of professionals in a number of fields intended to manage resources to reduce vulnerability to hazards and to cope with disasters that may have been created as a result of accidents, by individuals (such as terrorists or active shooters) or by nature (such as floods, earthquakes, tsunamis, or wildfires). The Incident Command System (ICS) facilitates managing these activities by integrating multiple agencies' facilities, equipment, personnel, procedures, and communications into a common organizational structure that is scalable to the size and type of emergency, is applicable across disciplines, and can be used to organize immediate and long-term field operations for natural or manmade incidents.

Introduction

Emergency management is not only about *responding* once an incident has occurred, it also includes the agencies and activities responsible for *protecting* against an event's occurrence, *mitigating* the consequences of and *recovering* from the event. Each step requires coordination among federal, state, tribal, local, and cross jurisdictional government agencies; educational and health-related institutions; utilities and communications providers; nonprofit, social service, and community-based organizations; and private companies. Emergency management focuses on measuring

and managing risk. Risk managers undertake assessments to consider the probability (likelihood) that an event will occur and its consequences (damage to people, property, or the environment and how much money, time, and other resources it will take for recovery). They may consider, for instance, the risk of a toxic chemical spill following a train derailment or truck accident; of a flood, tsunami, wildfire, or earthquake; or of an active shooter at a school or shopping mall. Once they have assessed the risk, they consider how to manage it, which includes developing an Incident Action Plan (IAP) should the event occur.

Individuals will assess risk and determine how to manage it daily, but do not think of it as risk management. If you avoid a part of town you believe is unsafe or if you decide not to take an umbrella when rain is predicted, you have assessed risk. In the first case, you are weighing the risk of becoming a crime victim, in the second, the likelihood of getting rained on. In both, you considered risk based on probability (how likely is it to happen) and consequence (how bad will it be). This entry describes the development of disaster relief and emergency management, explains the ICS protocols, and discusses the applicability of those protocols to different types of events.

Early Disaster Relief

The U.S. government's involvement in disaster relief is acknowledged to have begun on February 19, 1803, when Congress passed the Relief of Sufferers by Fire in the Town of Portsmouth [New Hampshire] Act to make federal resources available in response to a December 26, 1802 fire that devastated the town. The Act authorized "the Secretary of the Treasury to suspend, for a limited time, the collection of bonds due to the United States by merchants. . .who. . .suffered by the. . .conflagration. . ." (City of Portsmouth 2016, p. 7). This was required because Congress lacked authority to pass laws that applied to specific states (and by extension, areas within states). It was unconstitutional for Congress to allocate money from the Treasury or to suspend funds due the Treasury as a form of relief.

Between 1803 and 1950, Congress passed more than 100 ad hoc laws to provide relief or compensation to individuals or localities after disasters (Drabek 1991, p. 6). The 1950 Disaster Relief Act (DRA) (Public Law [PL] 81–875; amended in 1974 as PL 93–288) eliminated the need for event-specific disaster aid packages by creating a permanent, national disaster relief program and encouraging states to develop disaster plans (Yoshpe 1981, p. 523; Birkland 1997, p. 49) and it transferred the authority to declare a disaster from Congress to the President. Natural disasters in the 1960s and 1970s led, in 1974, to amending the DRA to allow the federal government to provide individual and family assistance after a disaster. A National Governors' Association (NGA 1978) report highlighted concerns that the federal government lacked a national emergency policy and that the large number of agencies assigned disaster responsibilities made it difficult for states to manage these events. The NGA advocated for greater state/local discretion in using federal funds and for a greater focus on prevention and recovery, rather than primarily on activities during a disaster.

National Incident Management System (NIMS) and the Incident Command System (ICS)

Upon creation of the Federal Emergency Management Agency (FEMA) in 1978 by President Jimmy Carter, its first permanent director, John Macy, tried to create an integrated emergency management system (IEMS) that would provide a multi-hazard approach, depended on professional management at the state and local levels (Greenstone 1989, p. 22), and could be used to manage nature-made disasters as well those created by intentional acts. This approach remains the basis of today's National Incident Management System (NIMS) and Incident Command System (ICS).

Also foreshadowing NIMS and ICS, Congress in 1988 passed the Robert T. Stafford Disaster

Relief and Emergency Assistance Act (PL 93-288 as amended; further amended by the Disaster Mitigation Act of 2000 and the Pets Evacuation and Transportation Standards Act in 2006). The Act, named for its chief sponsor, Sen. Stafford (R-VT), authorized the federal government to handle emergency assistance and response activities; increased cost sharing from a 50/50 ratio to 75 % federal/25 % state/local; expanded cost sharing to include public assistance programs; redefined the meaning of an eligible private, nonprofit facility, and authorized family grant and disaster housing programs. It places a limit on the President's ability to declare a disaster by specifying the federal government may become involved only after a state's or territory's governor has requested assistance. This may be overridden only when it is apparent the state is unwilling or unable to fulfill its basic governmental functions.

The Stafford Act formalized FEMA's role coordinating government-wide relief efforts and required local or tribal governments to develop disaster mitigation plans and to establish implementation strategies. States must also develop plans and must explain how they will support local/tribal governments in fulfilling their plans. Preparing for hazards must include creating preparedness plans, recruiting and training personnel, conducting research, stockpiling materials and supplies, creating warning systems, and constructing shelters.

Within less than a month after the September 11, 2001 terrorist attacks in New York City, Washington, DC, and Shanksville, Pennsylvania, President George W. Bush issued Executive Order 13288, which led to creation of the Department of Homeland Security (DHS). FEMA was one of the 22 federal offices and programs moved into DHS, where it is housed in the Emergency Preparedness and Response Directorate. Since March 2004, under Homeland Security Presidential Directive (HSPD) 5, *Management of Domestic Incidents*, states and territories must maintain an office of emergency management whose funding comes principally from FEMA and from the jurisdictions' budgets. These offices are often located in state offices of homeland security, where they coordinate emergency planning, disaster drills involving multiple agencies, and public outreach. To be eligible for disaster preparedness funds, federal departments and agencies; state, local, and tribal governments; the private sector and nongovernmental organizations (NGOs) must use NIMS to integrate domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan and they must employ ICS to manage on-scene response activities.

Similar to FEMA's concept of IEMS, NIMS is designed to help agencies define roles and responsibilities in an event and develop procedures to manage emergency operations. It is a template for agencies to work together during emergencies. It is intended to be flexible and scalable to allow agencies to plan for and respond to incidents regardless of cause, size, complexity, or location. ICS is an essential element of NIMS. Like NIMS, ICS is intended to provide a standardized approach to event management by outlining procedures that can be used regardless of an incident's type, location, duration, and the number and types of responding agencies. Many of the ICS protocols were developed in the 1970s by agencies fighting wildfires in California and other Western states. Because many of the agencies had never worked together, time and equipment were squandered, leading to the realization that they needed a coordinated approach such as ICS to bring personnel, equipment, procedures, and communications under a common structure to manage resources during and after an incident.

ICS is structured for activities in five areas: command, operations, planning, logistics, and finance/administration.

Command. ICS is based on the concept of unified command, which means that all responders work as a team under the same command structure and are not hindered by organizational boundaries that would require them to get direction only from their own agency (National Incident Management System 2014, pp. 11–12).

To assure that unified command is followed, key roles are defined. The Incident Commander (IC) is in charge and is responsible for all activities. In an incident, the first person on the scene is the IC until replaced by someone with higher rank

and/or greater expertise. Once the IC is identified, a unified command is established at the Incident Command Post (ICP) to which all responders report to receive their assignments. The Incident Commander should make the initial assessment of the situation unless relieving an earlier Commander. In that case, the oncoming IC must obtain a briefing from the IC being relieved. Once the IC has determined the incident's objectives and strategy, she/he must establish priorities and a Command Post (ICP) if it has not been previously established. After authorizing implementation of the incident action plan, the IC must assure that safety measures are in place; coordinate activity for all Command and General Staff and with key people and officials, and authorize release of information to the media. A key part of command authority is requesting additional resources or releasing of resources that are no longer required at the incident site, including ordering demobilization of the incident when appropriate.

A number of individuals make up the Command Staff, each of whom reports to the IC. These include the Liaison Officer, the Safety Officer, and the Public Information Officer (PIO). The Liaison Officer assures that personnel, regardless of their agency, receive similar instructions and are aware of their roles. The Liaison Officer assists the IC in maintaining contact with all the agencies involved in the incident, whether as responders or in some other role. This officer is responsible for identifying and minimizing miscommunications that may arise among agencies. The Liaison Officer may also advise officials not on the scene, including local government officials and senior personnel from the responding agencies, to assure that everyone receives the same information.

The Safety Officer is the senior safety official at the scene and is responsible for ensuring that safety, health, and environmental hazards are assessed. Assuring the safety of responders may include assessing and/or anticipating hazardous situations such as the presence of dangerous chemicals or whether a facility is structurally safe to enter. This officer is also generally responsible for assuring medical capabilities at an incident and coordinating with medical providers at the scene. A key role of the Safety Officer is to assure that all responders are accounted for before a scene is cleared. For example, at a train accident, the Safety Officer must assure that no one remains on the tracks before trains are permitted to resume service. In a fire or explosion, the Safety Officer assures no one is left behind in a smoldering or collapsed building.

The PIO interacts with and briefs the media and the public. Responders should not interact with the media; they should refer questions to the PIO. To assure a consistent message, ICS calls for establishing a Joint Information Center (JIC) with one PIO speaking for all the agencies. Because of the ubiquity of social media, a PIO may be assisted by someone who provides updated online information. In some circumstances, more than one PIO may be designated to speak on behalf of the IC. Generally, this occurs in a multisite situation where it is difficult for one person to be aware of what is happening at each site. A second PIO may also be assigned if the situation results in many victims or responders being taken to a medical facility, where a PIO may be located specifically to provide medical updates to the media. In any multiple-PIO situation, it is very important that the PIOs coordinate closely before releasing any information since inconsistent messages are likely to contribute to misunderstanding by the media and the public and could, in certain situations, cause confusion and even panic.

Operations. Operations personnel manage tactical operations at the incident based on the existing IAP – they are the actual responders. Operations section personnel manage the incident site to reduce the immediate hazard, including saving lives and property, establishing situation and site control, and restoring the situation to normal conditions. Incidents can include natural disasters such as wildlife or urban fires and floods; earthquakes; and hurricanes, tornadoes, or tropical storms. Other types of incidents are acts of terrorism or war-related disasters; hazardous materials sills, nuclear accidents; aircraft or train accidents; or public health or medical emergencies. While some incidents will require highly specialized operations responders, virtually all will include such operations personnel as fire,

law enforcement, and emergency services. Others might require assistance from public health or public works personnel, for instance, if many individuals must be treated at the scene or transported to area hospitals or if facilities must be blocked off or declared unsafe for occupancy. The Operations section is likely to also include individuals from private companies or non-governmental organization who have skills and qualifications beyond those held by public-agency personnel. This is why it is important that the planning process include not only public officials but also private sector managers who have access to personnel and equipment that many governments may lack either due to their small size or small budgets.

Planning. Planning staff collects, evaluates, and processes information to develop the IAP; this is likely to include an inventory of physical resources, specialized data, alternative strategies, and availability of specialists whose skills may be required to resolve an incident or for follow-up during recovery. Planning is a process that starts well before an incident takes places and continues long after the incident has been resolved. Almost all discussions of emergency management contain information on the planning function; while the descriptions might differ somewhat, the functions are always similar.

Different types of agencies may label the planning steps differently or break them into larger or smaller components, but generally planning covers the following steps.

Hazard analyses and capability assessments. A hazard analysis is a formal study of what might happen and what might go wrong in certain types of situations. It can be as basic as going through a facility to determine where hazards exist such as unsafe conditions or places trespassers could enter, or it could try to determine how likely a facility is to be an attractive terrorist target (possibly based on what type of product is produced there, or how important it is to the surrounding area as an economic or social resource, or what the publicity value would be to the terrorist organization in attacking that facility). Once a hazard has been identified, the likelihood of an event taking place must be considered but so must be a capability assessment, which requires the planners to ask themselves how capable their jurisdiction would be in preventing, responding, or recovering from an incident that might happen. These questions must be asked by the planners so they can consider what personnel, equipment, or other resources would be needed in the event the incident occurred.

Based on their assessment, the planners must now develop the IAP – what will the jurisdiction do if the incidents described in the plan or anything similar actually happens?

To assure that the IAP is viable, the knowledge, skills, and abilities that it relies on must be maintained. Generally, this is done through continuing education and training exercises. Agencies plan emergency response drills based on the type of incident they believe they might be faced with. For instance, transit agencies might have agency personnel train with federal, state, and local first responders to an exercise simulating a derailment, an active shooter situation at a train station or on a train, or an accident with multiple fatalities or a hazardous materials spill from a leaking freight car. Hospitals, schools, shopping malls, sports venues, and places of worship are more likely to have drills focusing on active shooters or hostage takers, although some might simulate terrorist activity if they believe they are likely targets. In all cases, the training activity should be based on a situation that could possibly occur at that type of facility since the goal is to measure the readiness of responders should such an event occur.

Based on the training event, planners and responders will evaluate the response. If there is a knowledge or capability shortfall (people do not know what to do or they lack the resources to do it), the planners must either re-evaluate the usefulness of their plan, making changes or developing strategies to bring the responders and materials up to what the plan calls for.

Demobilization. In the event of an actual incident, demobilization activities often fall to planners. In addition to assuring that resources are returned to their original source, planners are often responsible for collecting incident-related documents that must be reviewed with the goal

of assessing response. Like training events, documents, and post-incident reports will be used to reassess and revise an existing plan for future use.

Throughout these steps, the planners must consider where their resources will come from. Are there federal funds or other assistance available? What specialized skills exist within nongovernmental or private agencies? How would people be evacuated from their homes and where would they be temporarily housed? How close are area medical facilities and what resources do they possess or lack that would be important in a disaster emergency? Once this type of information is collected, reviewed, and evaluated, it must be shared with those who will be responsible for carrying out any activities. Planning is an ongoing process; the IAP will generally be reviewed and modified at least annually to incorporate changing conditions and changing resources.

Logistics. Logistics entails the coordination of complex operations that involve many people, facilities, or supplies, most often from more than one source. In a business environment, logistics is defined as managing the flow of how things get from their point of origin to the point of consumption, or where something is made or grown to where the customers are. In emergency management, logistics describes making sure that all resources are in place or will be available when needed. This means that logistics personnel are responsible for assuring that support needs are met; this will include facilities; transportation; communications; supplies; equipment maintenance and fuel; food and medical services for responders; and off-incident resources.

Logistics personnel play a key role in IAP development; they are often responsible for creating protocols to assure that support networks are in place. For instance, if certain types of vehicles or machinery are required for certain situations, what local agencies have them and how quickly can they be brought to the incident site? In mass injury events, it is crucial to know the distance to each area hospital and the capabilities of each to handle various types of medical emergencies. Logistics personnel also have an important role after an incident has been resolved since their recording of what agencies supplied personnel and equipment can be crucial to assure that compensation and claims are properly apportioned among the agencies and charged to FEMA, insurance agencies, or others responsible for reimbursement after accounts are reconciled.

Finance/Administration. Finance/Administration personnel provide financial and/or administrative services support to incident management activities. Because funds may come from many different sources and may be charged to different accounts within those sources, all incoming funds such as government grants or contributions from private sector participants must be recorded and tracked, as must be funds expended during an incident. In some instances, where it can be anticipated that certain equipment will be needed for certain types of incidents, a jurisdiction may decide to purchase the item; in such cases,[note bad margin break] Finance/Administration personnel are most likely to be responsible for disbursing the funds, controlling documentation of the purchase, and possibly determining where and how the equipment may be used under non-emergency conditions. They also manage the costs of an incident, including ensuring that responder costs (salary, overtime, travel vouchers, lodging, and meals) and any costs of purchases associated with response are accurate and complete.

Difficulties Assessing ICS in Different Types of Emergencies

Assessments of the benefits of ICS are mixed. Although ICS is used by agencies for many types of events, analyses focus on unusual or unexpected incidents (generally disasters) rather than on agencies' implementation of ICS for planned events. Agencies implement ICS protocols for concerts, parades, state or county fairs, or major sporting events (the World Series, the Super Bowl, or a marathon) but these rarely receive post-event attention unless major glitches occur. In addition, because discussions of ICS as an emergency management tool tend to focus on specific disasters rather than on ICS protocols generally, the analyses lack guidance on how to deal with the next disaster. The lack of general ICS assessment

is reinforced by post-incident (or after-action) reports, which normally gauge participants' response to *their* incident and how to improve *their* response, rather than on global concerns. Also, because responses to emergencies and disasters have political implications, politicians' post-event comments are likely to differ from the after-action reports of the participants and to contain vague promises of doing better next time rather than detailed policy discussions.

An example of this type of internal review occurred in Baltimore, Maryland, following demonstrations in April 2015 after the death of Freddie Gray while in police custody. The report noted that ICS was neither well-understood nor were NIMS principles adhered to by responding agencies. The after-action report found that authority of the Incident Commander (IC) was contested by senior members of the Baltimore Police Department (BPD); that the role of the emergency operations center (EOC – the name often applied to ICPs) was unclear and resulted in confusion to where responders should report to receive instructions despite policies outlining the EOC's role, that some agencies were unfamiliar with NIMS and ICS, and that many liaison personnel lacked the rank or authority to represent their agency. The report recommended assuring that the IC has full authority to manage an incident; that the location of the EOC be communicated to all responders and that expectations that all report there are reinforced, and that all agencies, particularly BPD, enhance ICS capabilities through training and more frequent utilization of ICS principles in routine incident management (Links et al. 2015, pp. 21–22). Although a decade apart, these findings echo comments in FEMA's Facilitator Guide to NIMS that "the most common cause of response failure is poor management" and that "confusion about who's in charge of what and when, together with unclear lines of authority, have been the greatest contributors to poor response" (FEMA 2004, pp. 2–2).

Generally, ICS has been deemed most successful among firefighting organizations (who were involved in developing it) and less successful with law enforcement, public health, and public works organizations (Baltic 2004). Others have pointed to successful implementation of ICS when events are confined geographically, when responding agencies share outcome goals, and when the agencies involved are familiar with ICS and familiar with each other. Two examples illustrate these observations.

The April 19, 1995 bombing in Oklahoma City, Oklahoma, that resulted in the collapse of the Alfred P. Murrah Federal Building left 168 people dead and hundreds injured after being set by anti-government militant Timothy McVeigh. ICS contributed to successful incident management because it was supervised from the start by the Oklahoma City Fire Department (OCFD), whose commanders were trained in ICS and who retained command throughout. The event involved primarily one heavily damaged building with a secure perimeter that called for skills urban search and rescue team and firefighters are trained to have. Although many of the responding agencies had not worked or trained together, they were familiar with and had participated in ICS training, and were able to use their knowledge to coordinate their response to the incident (Buck et al. 2006, pp. 7–8).

The Deepwater Horizon oil spill in the Gulf of Mexico presented a different set of challenges that undermined the benefits of ICS. This incident began on April 20, 2010 when a British Petroleum (BP)-operated well discharged an estimated 4.9 million barrels of oil into the Gulf before the well was declared sealed on September 19, 2010. Legal issues surrounding the case went on for years; in 2012, BP and the US Department of Justice settled criminal charges including BP pleading guilty to 11 counts of manslaughter, two misdemeanors, and lying to Congress, and agreeing to government monitoring of its safety practices. Additional payments were agreed to by BP in 2013, 2014, and 2015.

Analysts noted that competing goals and messaging by BP and the government agencies involved in the response prevented establishing either a unified command or unified messaging. In addition, many responders had little knowledge of and belief in NIMS and ICS protocols. Critics debated whether differing private and government goals may present inherent problems in

establishing the unity that ICS requires and whether the incident was spread over too large a geographical area for ICS to work effectively (McKay 2010). These examples point to problems relying on universal protocols that, although scalable and flexible, may not be elastic enough to meet all situations, particularly where there are conflicting goals or where responders have received little emergency response training.

Conclusion

Emergency management has developed from an ad hoc system of the federal government providing relief after a specific disaster to federal requirements that governments and NGOs have detailed IAPs that mandate use of NIMS and ICS protocols by responding agencies. While NIMS and ICS have added structure to emergency planning, response, mitigation, and recovery, reliance on the protocols has differed among agencies and types of incidents, and agencies employing the protocols have met with different levels of success. To counter this, in addition to encouraging greater training and relying solely on post-event analysis, government officials and emergency managers may need to recognize that the size and complexity of some events, as well as possibly conflicting goals among responders, may undermine ICS during some emergencies and that some modification of the ICS principles may be required to assure the high-level of emergency response that the protocols are designed to ensure.

Cross-References

- Emergency Management: Evacuations
- Emergency Management: Infant and Young Children Feeding in Emergencies
- Emergency Management: Pets
- Emergency Management: Recovery
- Homeland Security Act of 2002
- Natural Hazards
- Risk Analysis: National and International Standards

References

Baltic, S. (2004). The incident command system, long a fixture in the fire services, has increasingly migrated into law enforcement, other emergency and support services, and even the private sector. *Homeland Protection Professional,* January/February, no pages.

Birkland, T. A. (1997). *After disaster: Agenda setting, public policy, and focusing events*. Washington, DC: Georgetown University Press.

Buck, D. A., Trainor, J. E., & Aguirre, B. E. (2006). A critical evaluation of the incident command system and NIMS. *Journal of Homeland Security and Emergency Management, 3*(3). Article 1.

City of Portsmouth, NH. (2016). *Historical notes of fires, firefighters, apparatus, and events, June 1696 through December 2015* (5th ed.). NH: Fire Department.

Drabek, T. E. (1991). The evolution of emergency management. In T. E. Drabek & G. J. Hoetmer (Eds.), *Emergency management: Principles and practice for local government*. Washington, DC: International City Managers Association.

FEMA. (2004). *Facilitator guide, NIMS: An introduction IS-700.* Washington, DC: FEMA.

Greenstone, S.D. (1989). *Emergency management: A national perspective*. Fort Lauderdale: Report AD-A225-922 prepared for the FEMA.

Links, J., O'Connor, K., & Sauer, L.. (2015, December 4). *Recommendations for enhancing Baltimore city's preparedness and response to mass demonstration events (based on a review and analysis of the events of April 2015).* Baltimore: Johns Hopkins University.

McKay, J. (2010, September 13). Gulf oil spill prompts debate on NIMS, unified response. Available at: http://www.govetech.com/em/disaster/Gulf-Oil-Spill-Debate-NIMS-Unified-Response.html. Accessed 20 Jan 2019.

National Governors' Association. (1978). *Emergency preparedness project: Final report*. Washington, DC: NGA.

National Incident Management System. (2014, March 1). Washington, DC: Department of Homeland Security.

Yoshpe, H. B. (1981). *Our missing shield: The U.S. civil defense program in historical perspective*. Washington, DC: Defense Civil Preparedness Agency.

Further Reading

Bodiru, A. B., & Racz, L. A. (Eds.). (2014). *Handbook of emergency response: A human factors and systems engineering approach*. Boca Raton: CRC Press.

FEMA. (2017). *FEMA incident management handbook, B-761*. Washington, DC: FEMA.

ICS Resource Center. (2008, May). Washington, DC: Emergency Management Institute (EMI), FEMA. Available at: https://training.fema.gov.emiweb/is/icsresource

Ward, M. J. (2016, June 20). *NIMS incident command system field guide* (3rd ed.). Burlington: Jones & Bartlett Learning.

Emergency Management: Infant and Young Children Feeding in Emergencies

Sarah E. DeYoung
University of Georgia, Athens, GA, USA

Keywords
Infant feeding · Evacuation · Maternal and child health

Definition

The field of infant and young child feeding in emergencies (IYCF-E) is a set of practices, policies, and guidelines related to ensuring safe feeding of infants and young children during disasters and major hazard events.

Introduction

During large-scale evacuation and sheltering scenarios, families with infants need support for safe infant feeding. In the post-disaster setting, breastfed, bottle-fed, and mixed-fed infants require special care and support. Breastfed infants have a higher likelihood of survival in emergency scenarios (Jakobsen et al. 2003; WHO and UNICEF 2003; WHO 2015). Another benefit of breastfeeding is that infants are less likely to suffer from respiratory illness and other infections (WHO and UNICEF 2003). Breastfeeding improves health outcomes for women and infants (Rollins et al. 2016), and breastfeeding promotion provides resilience and protection for vulnerable groups in disasters (Gribble 2018). Distribution of commercial complementary foods (CCF) in emergency sheltering spaces can also be problematic because it may disrupt breastfeeding (early introduction of solids) and because the CCF may not contain the proper nutritional contents for toddlers and older children. Specifically, fortified complementary foods are nutritionally superior (Theurich and Grote 2017). Another issue for young children in emergencies is meal frequency and malnutrition during displacement and the post-disaster context (Sun et al. 2013).

Overview

Natural hazards, crisis and conflict, and other emergency settings can have adverse impacts on families with infants and young children. Breastfeeding is the safest form of infant feeding in disasters and emergencies and is the most cost-efficient intervention in vulnerable populations (Rollins et al. 2016). The context of the disaster event and access to resources are important in designing effective implementations for IYCF-E. For example, lack of access to clean water and supplies to sterilize feeding supplies makes safe bottle-feeding difficult in low-resource contexts, such as in a refugee camp (Gribble 2014; Prudhon et al. 2018). In high-income countries, lack of space in emergency sheltering facilities for breastfeeding, temporary interruptions in utilities, and other factors can pose challenges for families with infants (Callaghan et al. 2007; Gribble and Berry 2011). There are several factors that contribute to problems associated with poor IYCFE adherence. During disasters, media messages often contain myths of inaccurate information about infant feeding (Gribble 2013). These myths influence donor behavior and health workers' interactions with caretakers. These myths include (1) myths about milk/lactation "drying up" because of stress from the disaster event (e.g., DeYoung et al. 2018), (2) myths about maternal nutrition and breastfeeding, and (3) the myth of formula as essential. Another major problem that unfolds during disasters is the untargeted mass distribution of infant formula. This results in some families receiving breastmilk substitutes (BMS), although they were exclusively breastfeeding, and some families not getting the proper BMS. Other problems related to logistics may affect infant feeding. For example, in a mass-sheltering scenario, relief groups may distribute

formula without preparation instructions (and not in the user language).

Short-Term Sheltering

All efforts should be made by emergency personnel to keep families together, especially infants and mothers. Families should be assessed for feeding status at entry into emergency sheltering (bottle-feeding, breastfeeding, mixed feeding, combined with multiple children). Families that were exclusively breastfeeding before the disaster should be encouraged to continue breastfeeding the infant. A designated space for breastfeeding is essential for the caretakers and infants. A bathroom/toilet facility is not an acceptable space for designated breastfeeding. Families that require infant formula should have access to proper preparation instructions, space for bottle preparation, and access to sterilization supplies or disposable bottles and teats. Crisis communication messaging to shelter volunteers should include information about infant feeding guidelines. Infants requiring breastmilk substitutes (BMS) are at risk for food insecurity during emergencies. Therefore, all caretaker-infant dyads should receive support and assessments in sheltering and relocation locations.

Long-Term Displacement

Water and hygiene concerns are important for IYCF-E planning in long-term displacement settings. Diarrheal illnesses are the second leading cause of death of children under the age 5 (WHO 2015), and malnutrition and stunting severely impact infant health. Assessments of each mother-baby dyad to provide feeding support are essential. Relactation, cup feeding, and proper complementary feeding should all be considered when supporting families that are in long-term displacement situations. Mother-baby tent or space can provide a location for displaced families in mass-sheltering scenarios. These spaces may often overlap with other service providers such as psychosocial first aid or reproductive care and planning. Additionally, families should receive adequate age appropriate nutrition for toddlers and young children, such as whole fruits and vegetables. Beliefs, practices, and norms about infant feeding may vary across cultures and locations. Groups providing infant feeding support in emergencies should include cultural competency as a core part of their training and outreach activities. Having local community members as a part of the nutrition assessment team can build rapport with the families and create systems of capacity building (Murphy 2014) for the post-disaster recovery processes and in long-term humanitarian crises.

E

Conclusion

Implications for practice and policy: Emergency support functions should coordinate to support safe infant feeding. Specifically, mass-sheltering personnel should coordinate with nutrition and medical personnel to create consistent but flexible IYCF-E protocols. Additionally, increasing rates of baseline breastfeeding can improve health outcomes for families vulnerable to hazards and disasters. In complex humanitarian and long-term emergencies, humanitarian groups, in partnership with local governments of the affected area, should prevent mass distribution of BMS and CCF. Finally, proper steps should be taken to ensure that toddlers and small children have access to small but frequent meals that are highly nutritious.

Cross-References

- ▶ Emergency Management: Evacuations
- ▶ Emergency Management: Incident Command System
- ▶ Emergency Management: International

References

Callaghan, W. M., Rasmussen, S. A., Jamieson, D. J., Ventura, S. J., Farr, S. L., Sutton, P. D., & Posner, S. F. (2007). Health concerns of women and infants in times of natural disasters: Lessons learned from hurricane Katrina. *Maternal and Child Health Journal, 11*(4), 307–311.

DeYoung, S., Suji, M., & Southall, H. G. (2018). Maternal perceptions of infant feeding and health in the context of the 2015 Nepal earthquake. *Journal of Human Lactation, 34*(2), 242–252. https://doi.org/10.1177/0890334417750144.

Gribble, K. D. (2013). Media messages and the needs of infants and young children after cyclone Nargis and the WenChuan earthquake. *Disasters, 37*(1), 80–100. https://doi.org/10.1111/j.1467-7717.2012.01289.x.

Gribble, K. (2014). Formula feeding in emergencies. In *Handbook of dietary and nutritional aspects of bottle feeding* (pp. 587–590). Wageningen: Academic Publishers.

Gribble, K. (2018). Supporting the most vulnerable through appropriate infant and young child feeding in emergencies. *Journal of Human Lactation, 34*(1), 40–46.

Gribble, K. D., & Berry, N. J. (2011). Emergency preparedness for those who care for infants in developed country contexts. *International Breastfeeding Journal, 6*(1), 16.

Jakobsen, M., Sodemann, M., Nylén, G., Balé, C., Nielsen, J., Lisse, I., & Aaby, P. (2003). Breastfeeding status as a predictor of mortality among refugee children in an emergency situation in Guinea-Bissau. *Tropical Medicine & International Health, 8*(11), 992–996.

Murphy, J. W. (2014). *Community-based interventions: philosophy and action*. New York: Springer.

Prudhon, C., Benelli, P., Maclaine, A., Harrigan, P., & Frize, J. (2018). Informing infant and young child feeding programming in humanitarian emergencies: An evidence map of reviews including low and middle income countries. *Maternal & Child Nutrition, 14*(1), e12457.

Rollins, N. C., Bhandari, N., Hajeebhoy, N., Horton, S., Lutter, C. K., Martines, J. C., & Victora, C. G. (2016). Why invest, and what it will take to improve breastfeeding practices? *The Lancet, 387*(10017), 491–504.

Sun, J., Huo, J. S., Zhao, L. Y., Fu, P., Wang, J., Huang, J., & Yin, S. (2013). The nutritional status of young children and feeding practices two years after the Wenchuan earthquake in the worst-affected areas in China. *Asia Pacific Journal of Clinical Nutrition, 22*(1), 100–108.

Theurich, M. A., & Grote, V. (2017). Are commercial complementary food distributions to refugees and migrants in Europe conforming to international policies and guidelines on infant and young child feeding in emergencies? *Journal of Human Lactation, 33*(3), 573–577.

World Health Organization. (2015). *World health statistics 2015*. Geneva: World Health Organization.

World Health Organization, & UNICEF. (2003). *Global strategy for infant and young child feeding*. Geneva: World Health Organization.

Further Reading

Angood, C. (2017). Operational guidance on infant feeding in emergencies (OG-IFE) version 3.0. www.ennonline.net/operationalguidance-v3-2017.

Emergency Management: International

Jennifer Mincin
Health and Human Services Department,
SUNY Empire State College, Selden, NY, USA

Keywords

Humanitarian aid systems · International disaster management · International emergency management · International response systems

Definition

International emergency management is a complex system that includes response and recovery efforts that take place in countries with little or unstable infrastructure and lack of consistent resources.

Introduction

In this section, an overview of concepts relevant to international emergency management will be discussed to provide a foundation for understanding how conflict, natural disasters, and climate change affect different groups of people globally. In addition, a brief description of key international organizations will be reviewed. Responding to international emergencies requires tremendous communication, coordination, and execution on every level, from local resources, to regional, to international. As the world faces the looming threat of climate change and environmental degradation as a result of human behaviors, international crises become inextricably tied to increased natural disasters, less resources, and human conflict.

In general, the international community responds to emergencies in one of two ways: refugee and non-refugee. The United Nations has two separate mechanisms for response: the Refugee Coordination Model that focuses on

responding to refugee crises and the Humanitarian or Charter Approach that focuses on non-refugee crises. For example, the war in Syria created one of the largest refugee crises of the modern era. This crisis is considered a refugee emergency, so the UNHCR is the lead agency implementing refugee coordination, support, and response following the Refugee Coordination Model (see below). An example of a non-refugee emergency is the 2018 Indonesian tsunami and earthquake.

Refugee

There are an estimated 25 million refugees. The UNHCR defines a refugee as:

> [S]omeone who has been forced to flee his or her country because of persecution, war, or violence. A refugee has a well-founded fear of persecution for reasons of race, religion, nationality, political opinion or membership in a particular social group. Most likely, they cannot return home or are afraid to do so for fear of their lives. War and ethnic, tribal and religious violence are leading causes of refugees fleeing their countries (UNHCR n.d.).

In 1951, the Geneva Convention was signed, thus providing a definition of the term "refugee" and setting the UNHCR's broad mandate including the establishment of the three durable solutions:

1. Voluntary repatriation if it is safe to return (returning home)
2. Integration in host community (staying where they initially fled to)
3. Resettlement in a third location (in a country with a resettlement program generally)

The unfortunate reality is that most refugees experience a protracted situation, and returning to their homeland is too dangerous or simply not feasible. Each State (or country) determines how it defines refugee and asylees; therefore there are several various terms of refugee and where a country will allow admittance. For example, the United States may recognize Tibetans as refugees, but China does not (see Table 1: case study of Tibetan people, Fig. 1). The rights of refugees center around five key concepts:

Non-refoulement. Under international refugee law, States are "obligated" to not "refoul," or return, a refugee to their country of origin if it is still unsafe (their safety, life, or freedom were still under threat) (1951 Convention, art. 33(2)).

Freedom of Movement. Technically, refugees should be granted the ability to live in freedom and to be able to move freely in the place they have fled.

Right to Liberty and Security of the Person. While seeking asylum, refugees have the right to be secure and be safe and the right to liberty. Many countries detain asylum seekers, so this is meant to be a protection for them.

Right to Family Life. The family is seen as the "natural and fundamental group unit of society and is entitled to protection by society and the State" (International Covenant on Civil and Political Rights, art. 23(1)). This right essentially states that refugee families should stay together.

Other Rights. The 1951 Convention also protects other rights of refugees, such as the rights to education, access to justice, employment and other fundamental freedoms, and privileges similarly enshrined in international and regional human rights treaties.

Despite these rights being protected in the 1951 Convention and under human rights treaties, refugees in various countries do not enjoy full or equal legal protection of fundamental privileges (Mincin 2012). In the next three sections, issues faced by refugees – namely, asylum, statelessness, and displacement – that directly impact on international emergency management strategies and decisions are discussed.

Asylum

For a person to claim asylum in a country outside the individual's country of origin, an asylee must prove a well-founded fear of imprisonment, torture, or threat to life if they are returned to their country of origin. Persecution may be based on things such as violence (mental or physical), legal or law enforcement punishment (1951 Convention; Council of Europe), forced participation in criminal military service, violations based on gender (or gender-based violence), etc. In addition, well-founded fear and persecution can be based on the individual's race, religion, nationality, or political opinion or

The tensions and territory and land disputes between China and Tibet have a long history dating back to the end of the British colonial rule in the eighteenth century (Hess 2009). However, in 1950, the China invaded Tibet resulting in the Tibetan leader the Dalai Lama being forced into exile by 1959 (Doshi 2017; Hess 2009). The Tibetan plateau holds vast amounts of water reserves that China can harness for energy and other resources (Doshi 2017). In addition, Tibet boarders India making the geopolitical aspect to occupying Tibet an interest to the Chinese Communist government (Doshi 2017). The Dalai Lama has yet to return to Tibet and since 1959 has been leading the Tibetan Government in Exile in Dharamsala, India. For Tibetans who remain in China, they face fierce persecution, limited autonomy (or movement), and are forbidden to practice their religion (Buddhism) or have pictures of their political and spiritual leader, the Dalai Lama. The China-Tibet conflict is often viewed as an ethnic and/or religious conflict. This is understandable, given the prominence of ethnicity and religion in the conflict. Many Tibetans are Buddhists, while ethnic Han Chinese are generally not (Hess 2009). In addition, the Chinese government has a history of persecuting religious movements, especially those which draw large numbers of followers and which have the potential to transform into political movements that could potentially threaten the regime's hold on power (Hess 2009).

The situation in Tibet remains oppressive for Tibetans who still live there as there are reports of human rights abuses and persecution (Nickerson 2018; Doshi 2017; Dolma et al. 2006; Crescenzi 2002). For Tibetans who fled their country, the situation had created a profound sense of loss of home, nationality, and cohesion as an ethnic group (Nickerson 2018). The United Nations has not yet determined Tibetans are refugees; China is a major political player in terms of security, global economy, and power (Dolma et al. 2006). While land claims continue to be debated and the appetite to challenge China on-behalf of the Tibetan people non-existent, the United States and other major country still do not officially recognize Tibet as independent; they recognize Chinese sovereignty over Tibet. Recently, India has begun to offer Tibetans living in India Indian passports and pathways to citizenship (Nickerson 2018; Doshi 2017). Returning to their homeland seems like a distant dream for Tibetans.

Additional Resources on the Tibet and Human Right

1. Tibet: The Forgotten Refugee Crisis – https://www.dailysignal.com/2015/10/23/tibet-the-forgotten-refugee-crisis/
2. BBC Tibet Profile – https://www.bbc.com/news/world-asia-pacific-16689779
3. A State within a State: Tibetans in Nepal – https://thediplomat.com/2016/07/a-state-within-a-state-tibetans-in-nepal/

For Discussion

1. Are Tibetans refugees or stateless? Why? Why not?
2. What would an international disaster response look like in this scenario? Is it a refugee-based response or a non-refugee-based response?
3. How does this differ from a United States response and recovery effort?

Emergency Management: International, Fig. 1 Case study. The Tibetan people: stateless or refugees?

membership in a particular social group. There are currently 3.1 million asylum seekers, a number far greater than the capacity for any one agency to help them (UNHCR, Figures at a Glance 2018).

Stateless

According to the UNHCR, at least ten million people worldwide have no nationality (UNHCR, Figures at a Glance 2018). Most people who are stateless are stateless through no fault of their own; they are victims of circumstance. Statelessness – not having a nationality – occurs because of discrimination against certain groups, redrawing of borders, and gaps in nationality laws. The constant in all of this is that someone without a nationality cannot live the same life as someone with a nationality. For example, if you are stateless, you cannot get an identification card or bank account, access services in most areas, travel (since you will likely not have a passport), or do things common to most people such as enroll in school since there is no proof of nationality. Imagine a lifetime of obstacles and disappointment and imagine ten million people who

cannot achieve their full potential. The international legal definition of a stateless person is set out in Article 1 of the 1954 Convention relating to the Status of Stateless Persons, which defines a stateless person as "a person who is not considered as a national by any State under the operation of its law." This means that a stateless person is someone who does not have a nationality of any country. Some people are born stateless, while others become stateless over the course of their lives.

Internally Displaced Persons (IDPs)

There are an estimated 40 million internally displaced persons (IDPs) (UNHCR, Figures at a Glance 2018). IDPs are individuals who have been forced out of/fled their community, village, or neighborhood but remain within the boundaries of their country of origin. Therefore, they remain within the "protection" of their home country but cannot return back to where they live. IDPs are considered among the most vulnerable in addition to stateless people because they lack protection from their country of origin, and yet they are under attack. Climate change, large-scale drought, and loss of livelihood as a result of climate change are some reasons, in addition to internal conflict and persecution, that affect IDPs. Agencies trying to help IDPs are overwhelmed by the combination of sheer number of people requiring aid, lack of funding, and disorganization incurred when people leave suddenly without a plan for how to survive.

International Context

The United States is a part of a global emergency management community whereby similar agreements that exist within the United States also exist internationally including mutual aid, coordinated response efforts, and short- and long-term assistance. The field of emergency management exists throughout the world with some oversight by the United Nations and key response organizations. This entry is designed to provide professionals a foundational understanding of how international emergency management functions as well as provide an overview on core concepts and systems that enable a global, humanitarian response to crises, conflict, and disasters. When considering international disaster management, it is important to understand that often response and recovery includes working in conflict areas and the aftermath of natural disasters (Collins 2018; Phillips et al. 2017). In the United States, we are more familiar with natural disasters and mass violence. For example, while the United States has high rates of gun violence, mass shootings, and riots, they are currently not on the scale of what is experienced in other parts of the world as wars are generally fought overseas. In addition, while the United States is experiencing the effects of climate change (such as more extreme weather and wildfires), other nations experience famine as a result of drought and disease outbreak in greater severity. Phillips et al. (2017) point to the 2014 Ebola outbreak as an example. Thousands of people died as a result of the 2014 Ebola outbreak primarily in Sierra Leone and Liberia. In the United States, one person died (Phillips et al. 2017).

International emergency management is implemented in times of crisis. While, at times, the international community will distinguish between a conflict response as humanitarian aid and a response to natural disasters as international emergency management response, those distinctions are fading as the emergency management community recognizes that disasters occur from both human-made and natural effects. The context may be different in Yemen than in Indonesia after a tsunami, but the emergency response needed to help people recover tends to be the same (Bullock and Haddow 2003; Phillips et al. 2017). Further, climate change is increasing the impacts of both conflict (as resources become scarcer around the world, the risk of conflict and war increases as well) and natural disasters (such as drought caused by over-farming and deforestation) (International Organization on Migration, Migration, and Climate Change n.d.). Consider the statistics. Globally, there are an estimated 68.5 million people who have been forced to flee (UNHCR, Figures at a Glance 2018), a number that has surpassed the number experienced during World War II (UNHCR, Figures at a Glance 2018). Currently, the world is seeing the largest

number of forced migrations from conflict alone. The World Bank estimates there could be 148 million climate migrates in the coming years (International Organization on Migration, Migration, and Climate Change n.d.; Parker 2018; Spiker et al. 2018).

A compelling factor in international disaster management is the fact that there are over 195 countries in the world today with 193 participating members (or member states) of the United Nations (World Atlas, How Many Countries are There in the World 2018), thus making standardization, coordination, oversight, and mandatory practice challenging. Part of understanding how international emergency management functions includes understanding the legal frameworks, working groups, and mechanisms that enable humanitarian aid to work. This includes power dynamics, inequality, and globalization and the intersection of crisis, conflict, and oppressed groups. In addition, it is important to understand the international legal definitions and frameworks that essentially enable the international disaster system to function, of which the United States is a part of. The foundation of international disaster response is the notion that all people are deserving of assistance during emergencies and crises in a dignified manner and with integrity placing the person first. According to the International Federation of Red Cross and Red Crescent, NGOs agree that humanitarian aid must be delivered to all people without impediment and that "[a]id is given regardless of the race, creed or nationality of the recipients and without adverse distinction of any kind" (DRC n.d., bullet 2). The next section describes the roles and responsibilities agencies play in international disaster management.

Agency Roles and Responsibilities

International Nonprofit Organizations/ Nongovernmental Organizations

Similar to the history of disaster response and recovery organizations in the United States, there are several international relief organizations. Some agencies are well known, such as the International Red Cross, Medecins Sans Frontieres (MSF or Doctors Without Borders), and Save the Children. Others are less known, but equally as important in terms of providing much needed assistance often in unsafe conditions. These may include Mercy Corp, Islamic Relief, and BRAC, an organization that assists with humanitarian relief as well as development. International nonprofits, also referred to as international nongovernmental organizations (INGOs), are private, nongovernmental organizations. Generally, INGOs have multiple chapters or offices throughout the world and function as a large-scale operation. INGOs are not considered local community-based organizations, though often work closely with local organizations during response and recovery. INGOs are lead organizations within the United Nations response system (see section below) and tend to have a lot of capacity and resources when it comes to logistics and person-power. For example, the MSF has a stockpile of supplies ranging from vaccines to basic food and water. This stockpile can be deployed rapidly at almost any time.

Community-Based, Faith-Based, and Ethnic-Based Community Organizations

As the name indicates, community-based organizations (CBOs) are nongovernmental, private nonprofits run locally and fully embedded in communities. Ethnic- and faith-based organizations are similar to CBOs but are primarily focused on specific ethnic or faith communities. That essentially means they are founded in a specific faith or ethnicity but may provide services outside the specific faith or ethnicity (McKnight and Plummer 2015; Phillips et al. 2017; Mincin et al. 2013). While CBOs, FBOs, and ECBOs may have less capacity in terms of funding, person-power, and resources, they are crucial partners during emergencies. CBOs/FBOs and ethnic community-based organizations (ECBOs) have deep relationships with the people in affected communities and can assist with culturally appropriate responses, emergency program planning, and implementation and assist with communications and coordination on the ground. Perhaps the most critical role CBOs and ECBOs play is in ensuring the local language, culture,

religion, and context are not only taken into account but fully integrated into every aspect of emergency response planning and relief work. Large, international organizations do make efforts at hiring people from the community in local offices; however response teams may include people from Europe and the United States. It is not enough to have cultural competence, and it may be difficult to deeply learn about and fully understand specific cultures, languages, religions, and ethnicities during rapid deployments. Working closely with and allowing local organizations and community leaders and members to take the lead in terms of response and program development and implementation is vital.

When aid workers are deployed to the Ceylanpınar refugee tent camp located in Turkey just along the Turkey/Syrian border (UNHCR 2018), it is necessary for them to understand the Syrian conflict and why so many have fled, but also to understand gender roles, the majority religion practiced, and cultural practices for Syrian and Turkish people (Phillips and Thompson 2013). It is the job of the aid worker to be as nonjudgmental and humble as possible when delivering aid in a foreign country (Phillips et al. 2017). It is only logical and correct, then, to allow local community- and faith-based leaders to lead in implementation and navigation of systems and cultures. Further, aid workers can learn from community members and leaders while on deployment. Cultural sensitivity and respect are paramount, but the willingness to be open to learning about and sharing in the experiences of the community you are working with during a response is equally as important. This informs delivery of services, ensures continuity when the response moves into the recovery phase, and assists aid works on future deployments. In the example of aid workers being deployed to Ceylanpınar, there are not only likely differences between refugees in the camp and aid workers who come from all over the globe, there are cultural practice differences between people from Turkey and Syria. One cannot simply assume that because it is the same geographic region or that there is a shared religion (as is the case for Islam) that practices and cultures are the same (Dalal 2017). In addition, within Syria, there are distinct ethnicities and religions including the Bedoin, Sunni Muslim, Shia Muslim, and Assyrian Christians (Dalal 2017; Kannike 2019).

United Nations High Commission on Refugees (UNHCR)

The UNHCR was officially established in 1950 (UNHRC n.d.), initially with a 3-year mission post-World War II. However, in 1956, Soviet forces invaded Hungary, stopping the revolution. At that time, the permanency of the UNHCR was established (UNHCR n.d.). Generally, the UNHCR oversees activities as it relates to international conflict, humanitarian aid, international emergency management response, and protections. However, there are two additional entities that oversee North Korean asylum and Palestinians receiving aid; they are the United Nations Korean Reconstruction Agency (UNKRA) and the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), respectively (UNHCR n.d.).

United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA)

The UNOCHA is one of the lead coordinating agencies active in complex, global international responses. It was initially formed in 1991 to ensure coordinated, efficient, and coherent response to humanitarian crises (UNOCHA, Who We Are n.d.). OCHA:

> carries out its coordination function primarily through the IASC, which is chaired by the ERC. Participants include all humanitarian partners, from United Nations agencies, funds and programs, to the Red Cross movement and NGOs. The IASC ensures inter-agency decision-making in response to complex emergencies. These responses include needs assessments, consolidated appeals, field coordination arrangements and the development of humanitarian policies (para. 16).

OCHA provides funding, recourses, coordination, and human power in times of crisis and emergency response. It is a central international agency in terms of international disaster response.

United States Agency for International Development (USAID)

Founded by President John F. Kennedy in 1961, the USAID leads the US international humanitarian aid responses and international development initiatives. The Office of US Foreign Disaster Assistance (OFDA) is the office within USAID, which oversees the Disaster Assistance Response Team (DART). The OFDA is responsible for the deployment of resources and relief workers globally. DART can be deployed anywhere in the world including here in the United States. For example, in 2017, DARTS responded to the earthquake in Mexico and Hurricanes Irma and Maria in the United States (OFDA 2017; USAID, Caribbean Hurricanes n.d.). In the next section, an explanation of the effects of changes in both environment and climate on the role of aid workers is provided.

Environmental Degradation and the Effects of Climate Change

According to USAID, over the last 60 years, the world population went from 2.5 billion people to over seven billion, increasing the demand for ever-shrinking resources and conflicts that stem from resource control. Exacerbating the situation is the use of fossil fuels and rapid deforestation (USAID, Environment and Global Climate Change 2018). Climate change is creating more fierce and intense weather events and, as resources shrink, perpetuates wars and conflicts as people fight over control of those resources. The International Association of Emergency Managers recognizes the importance and severity of climate change. In 2015, IAEM released a statement stating:

> Ongoing climate change affects all regions, generating not only direct public-safety hazards, but also long-term economic, sociological, and public-health impacts. IAEM-USA strongly recommends comprehensive mitigation and adaptation strategies, integrated with existing processes such as hazard and land-use planning, as the only realistic path for resilience among individuals, communities, and our nation. In addition, IAEM-USA specifies that emergency managers have a critical role in this process and should be considered essential participants at all levels of government (IAEM, The Critical Role of Emergency Management in Climate Change Planning, 2015).

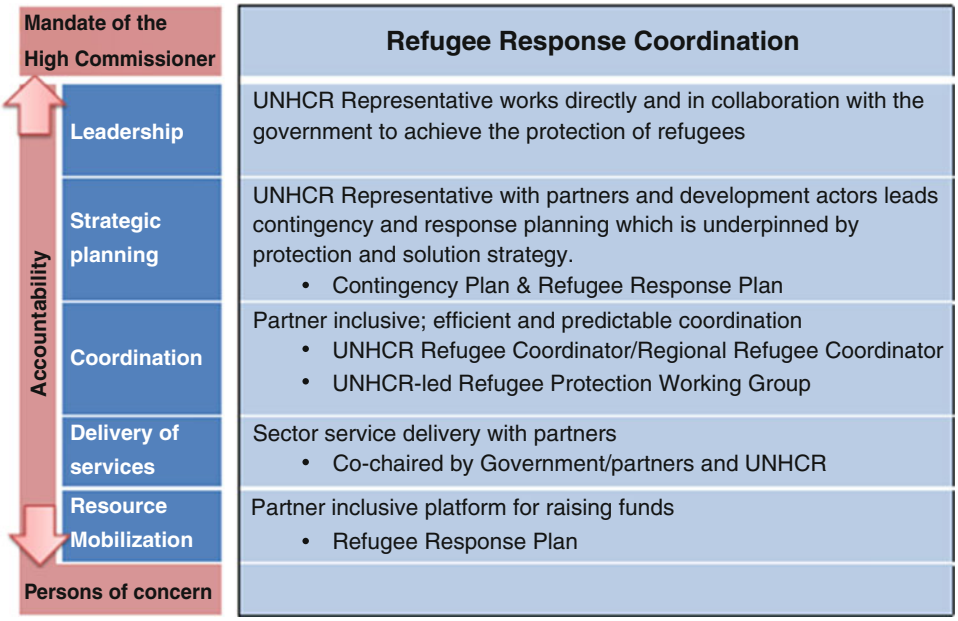
Environmental degradation and climate change have had a significant impact on migration flows, refugees, IDPs, and other vulnerable populations. This creates increased complications on humanitarian aid workers and international disaster response and recovery systems (Coppola 2015). In addition, climate change disproportionately affects the most vulnerable populations including people with disabilities, the aging, people living in poverty, women and girls, and ethnic and racial minorities (Levy and Patz 2015). Levy and Patz (2015) stated, "Environmental consequences include increased temperature, excess precipitation in some areas and drought in others, extreme weather events, and increased sea level" (p. 310).

Frameworks and Governance

This section discusses key, governing agencies active in response and recovery during humanitarian crises. Humanitarian crises may include both human-made (war, conflict, terrorism, technological) and natural (tsunamis, earthquakes, hurricanes/cyclones). UNHCR, international non-governmental organizations, and community-based organizations play a key role in coordinating response and recovery as well as planning and preparedness. In addition, and especially community-based organizations, play a pivotal role in advocacy both country-wide and internationally.

Refugee Coordination Model

Given the scope and often protracted nature of refugee crises, there is a specific system overseen by the UNHCR to facilitate response and recovery during refugee crises (the Refugee Coordination Model (RCM) shown in Fig. 2). The country or countries who are receiving refugees are called the "host country." When the host country becomes overwhelmed, the RCM and the UN High Commission on Refugees (UNHCR) will


Mandate of the High Commissioner
Persons of concern
Accountability
Refugee Response Coordination
Leadership
UNHCR Representative works directly and in collaboration with the government to achieve the protection of refugees
Strategic planning
UNHCR Representative with partners and development actors leads contingency and response planning which is underpinned by protection and solution strategy.
• Contingency Plan & Refugee Response Plan
Coordination
Partner inclusive; efficient and predictable coordination
• UNHCR Refugee Coordinator/Regional Refugee Coordinator
• UNHCR-led Refugee Protection Working Group
Delivery of services
Sector service delivery with partners
• Co-chaired by Government/partners and UNHCR
Resource Mobilization
Partner inclusive platform for raising funds
• Refugee Response Plan

Emergency Management: International, Fig. 2 Refugee response coordination

coordinate a refugee response effort. According to the UNHCR RCM, "Primary responsibility to protect refugees rests with states. Coordination of the refugee response is determined by capacity and approaches of host government and builds on resources of refugees and hosting communities" (p. 1). For example, when the war in Syria started, thousands of refugees fled. Greece became a host country. Greece tried to provide as much support to the refugees seeking safety, but because the country was deeply affected by the financial crisis of 2008, Greece was still grappling with economic instability. Eventually, UNHCR provided support along with nongovernmental agencies such as the International Rescue Committee, Save the Children, and Medecins Sans Frontieres (Doctors Without Borders).

Sphere

The *Sphere Handbook* came about as an effort to bring the humanitarian community together in terms of services, protection of refugees and displaced populations, and preservation of life and dignity. It is an attempt at standardizing practices, increasing accountability, ensuring no further harm, and monitoring and evaluating. There are several participating agencies that have dedicated ample amount of time writing, updating, and implementing the standards laid out in Sphere. However, there remain issues around implementation of the standards of practice, accountability, and consistency; it is still a critical and important document and effort. It lays the groundwork in terms of shifting how humanitarian response is done and attempts to raise the bar regarding services provided and accountability.

The Sphere Project was initiated in 1997 by a group of NGOs and helped to establish the *Humanitarian Charter and Minimum Standards in Humanitarian Response Handbook* to clarify ethical roles, responsibilities, and accountability of humanitarian aid workers and to promote set, minimum criteria that put the care and empowerment of the beneficiaries first. According to the handbook's foreword:

> The Humanitarian Charter and minimum standards will not, of course, stop humanitarian crises from happening, nor can they prevent human suffering. What they offer, however, is an opportunity for the enhancement of assistance with the aim of making a difference to the lives of people affected by disaster (Sphere 2018, p. iii).

The Sphere Project has two core beliefs: (1) people affected by crisis have a right to a life with dignity and a right to assistance during the crisis and (2) "that all possible steps should be taken to alleviate human suffering arising out of disaster or conflict" (Sphere 2018, p. 4). At the core of Sphere is the philosophy that "all people have the right to safety, security, and a life with dignity" (p. 4). The Humanitarian Charter provides the ethical and legal backdrop to the core standards and protection principles and lays out nine core standards (see Core Humanitarian Standards chart). The core standards focus on people-centered approaches and response, which is largely based on a strengths-based approach to working with clients. The strengths-based, or resiliency, approach has long been used in disaster mental health, trauma, and crisis settings. The strengths-based approach, or strengths perspective, was developed by Saleeby (1996) as a different approach from the more diagnostic model (Mattaini and Lowery 2007).

According to Saleeby (1996), the strengths-based approach developed as a technique in working with people with severe mental health conditions and has since grown to work with other vulnerable populations such as the elderly, youth at risk, and even communities. It also is closely aligned with resilience, wellness, integration, and psychosocial approaches. This approach is used in both domestic disaster response and international and can be applied in conflict zones as well as natural disaster responses. The strengths-based approach, like integration, takes the prior information a refugee brings with him or her as a part of the full intake process. Therefore, information on where the refugee has been; what he or she has been exposed to and survived, known, or understood; chronic ailments; family dimensions and dynamics; and the political and social structure of the homeland all come into relevance (Ryan et al. 2008).

Sphere also focuses on agency coordination and collaboration ensuring different organizations are working together on the ground and globally. Assessment includes standardized ways of doing on-the-ground assessments during crisis as well as pre-disaster information. In addition, standardized ways of designing programs (case management, psychosocial, health clinics, food distribution sites, shelter management, etc.) and response as well as focusing on organizational transparency and accountability are a part of the core standards. Aid worker performance is usually implemented at the individual agency level (Fig. 3).

The Cluster System and Interagency Standing Committee

Established in 1992, the IASC is an "inter-agency forum for coordination, policy development and decision-making involving the key UN and non-UN humanitarian partners" with the goal of strengthening humanitarian assistance. The Cluster System, established in 2005, is a coordination approach established by the United Nations and international nongovernmental organizations as a means of ensuring coordination and effective rapid response during emergencies, crises, and disasters. The Cluster System is activated for non-refugee crises. Within the Cluster System, there are "lead" agencies that agree to be the lead coordinators during humanitarian emergencies (see Fig. 4, "The Cluster Chart").

Globalization, Power Dynamics, and Humanitarian Aid Systems

In this section, we will have a brief discussion on the intersection of race, gender, ethnicity, poverty, and environmental degradation as it relates to humanitarian aid systems and international disaster management and relief. For example, refugees around the world are perhaps one of the most vulnerable groups because many have been forced to flee their homes, often at a moment's notice, and have been dislocated with nothing more than the clothes on their backs. Some refugees may be fortunate enough to have received an education before they were forced to flee (such as many Iraqis) or placed in refugee camps (such as some Burmese). They must fend for themselves in environments of poverty, discrimination, lack of access to healthcare and education, and by living in a refugee camp or urban environment that often

Core Humanitarian Standard • Core Humanitarian Standard • Core Humanitarian Standard • Core Humanitarian Standard •
1
Humanitarian response is appropriate and relevant.
2
Humanitarian response is effective and timely.
3
Humanitarian response strengthens local capacities and avoids negative effects.
4
Humanitarian response is based on communication, participation and feedback.
5
Complaints are welcomed and addressed.
6
Humanitarian response is coordinated and complementary.
7
Humanitarian actors continuously learn and improve.
8
Staff are supported to do their job effectively, and are treated fairly and equitably.
9
Resources are managed and used responsibly for their intended purpose.
Humanity
Impartiality
Neutrality
Independence
Communities and people affected by crisis

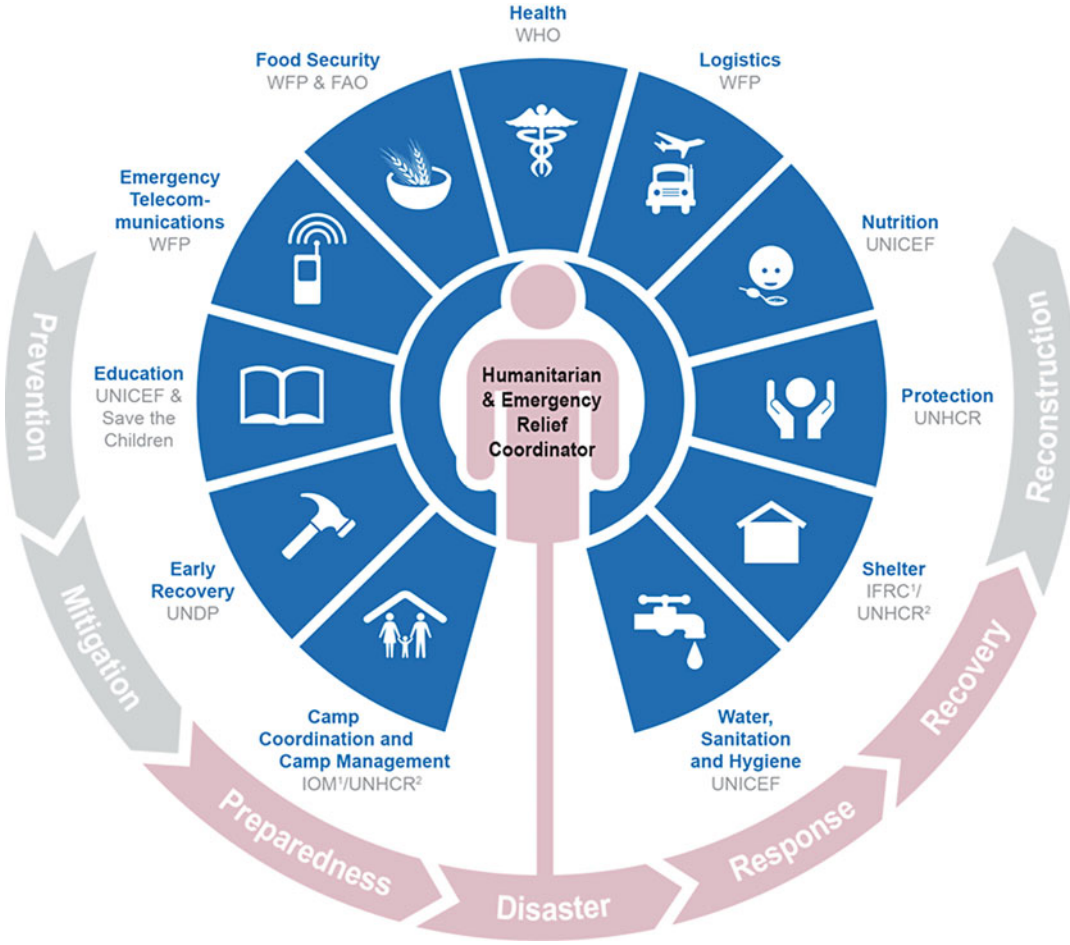
Emergency Management: International, Fig. 3 Humanitarian core standards

is not welcoming to them. Many languish in camps for years even though the refugee assistance community has learned that—once given certain opportunities—they can thrive (Mincin 2012, Mincin and Phillips 2017).

According to the Federal Emergency Management Agency's International Disaster Management, Chap. 13: International Emergency Management (2013) stated:

> The capacity to respond to large disasters achieved by individual nations can be linked to several factors, including propensity for disaster, local and regional economic resources, organization of government, and availability of technological, academic and human resources. However, it is becoming increasingly common that the response ability of individual nations is insufficient in the face of large-scale disaster, and outside assistance must be called upon. The greatest incidence of natural disasters occurs within developing countries, with 90% of disaster-related injuries and deaths sustained in countries with per-capita income levels that are below $760 per year (p. 2).

The Ebola outbreak of 2014 (see Table 2, "Case Study 2014 Ebola Outbreak", Fig. 5) is an example of how developing countries are more vulnerable and at higher risk for death and disruption from emergencies and crises. Developing countries, such as Liberia and Sierra Leone, do not have robust, functional healthcare systems, and strong infrastructure. When a crisis occurs, the response community must contend with moving materials and relief workers to the location (logistics) as well as establish relief centers. When physical infrastructure (roads, hospitals, clinics, etc.) are either not established or sparse and basic to begin with, the effects of response are immediate.



Emergency Management: International, Fig. 4 The cluster approach, IASC

Conclusion

As this entry demonstrated, international emergency response is complex due to the large number of organizations involved in several aspects of relief work. The field is vast and complex, requiring refugee humanitarian response to be coordinated by a separate UN entity. Both refugee and non-refugee emergencies require cooperation and resource sharing from government and non-government agencies. Research indicates that effective aid and long-term solutions are still inadequately resourced at a time when we face conflicts globally and climate change (Disaster and Climate Change 2019; Mahmood 2015; Ferris 2014; Harmer and Macrae 2004; Beeler 2018). Estimates for aid are staggering. For example, it is estimated that 22 million people in Yemen are in need of aid (Philip 2018); in Afghanistan about the same number of people who have been displaced from conflict have also been displaced by drought caused by climate change (Morse/IRIN 2019); and, there are over five million Syrian refugees and over six million displaced Syrians (Morse/IRIN 2019). In fact, OCHA estimates that over 135 people around the world are in need of some form of aid as a result of natural disasters, conflict and war, and the effects of climate change (OCHA 2018). Organizations writ large need to consider the complex interplay between climate change, conflict, natural disasters, poverty, race, and gender

In 2014, the world saw the largest Ebola outbreak in history (Centers for Disease Control 2017). Ebola is a deadly virus that can quickly spread via body fluids especially in conditions where communities do not have access to basic hygiene. According to a report by Save the Children, over 23,000 people contracted Ebola, and over 11,000 people died with 433 of them healthcare workers responding to the health emergency (CDC 2017; Wright and Hanna 2015). The tragedy of the Ebola outbreak was in part because of fragile health systems in West African countries as well as the international community's slower than usual response (MSF 2014; Saxene 2014). Guinea, Liberia, and Sierra Leone experienced the worst of the outbreak and were hardest hit with those infected and loss of life. As a result of the countries having weak health systems, Ebola was not contained, and the local and national response systems quickly overwhelmed (Wright and Hanna 2015). Compounding the situation is the fact that those most vulnerable and located in more remote and poor areas were hardest hit and lacked access to health services and education (Wright and Hanna 2015). In addition, women (especially pregnant women) and children were at greater risk.

Key US-based organizations assisted in the response in-country including the USAID and the CDC. In order to stem the spread of the disease, stronger surveillance systems needed to be put in place as well as in-country bolstering of healthcare workers and aid workers (CDC 2017). The USAID deployed the DART (Disaster Assistance Response Teams) in coordination with the UN and the World Health Organization (WHO). International relief organizations responded as well including the Medecins Sans Frontieres (MSF), the International Rescue Committee (IRC), and Save the Children among others. Although relief organizations alerted officials locally and internationally early on in the epidemic, the alert was not acted upon immediately according to some organizations (Gegout 2015). Among lessons learned from the response included: listen to nongovernmental organization alerts and assessments, improve health systems and facilities in-country, plan logistical responses to health emergencies better, and fund pharmaceutical research (Gegout 2015; Wright and Hanna 2015).

Additional Resources

1. Save the Children: A Wake up Call – https://www.savethechildren.org.uk/content/dam/global/reports/health-and-nutrition/a-wake-up-call.pdf
2. Key Events in the WHO Response to the Ebola outbreak – https://www.who.int/csr/disease/ebola/one-year-report/who-response/en/
3. 6 Lessons Learned from the international Response to Ebola – https://www.weforum.org/agenda/2015/02/6-lessons-from-the-international-response-to-ebola/

For Discussion

1. What aspects of the Cluster System gets activated in this scenario?
2. What is the role of the United States? Which US agency would be the lead?
3. What type of an emergency was the Ebola Outbreak considered?
4. What key factors aided in the spread of Ebola and death toll?
5. Think about the United States role in these types of emergencies. How does mutual aid assist locally and globally? How can the United States not only assist during response but in the recovery phase as well?

Emergency Management: International, Fig. 5 Case study. 2014 Ebola outbreak

as aid workers continue to meet the growing challenges of displacement. In addition, a push toward local solutions, empowerment, and resiliency building may be a part of the solution. However, resources, support, technical training, and funding need to be made available to local community organizations.

This entry provided an overview of key response agencies, response mechanisms and systems, definitions and roles and responsibilities, and the global context. Emergency managers are encouraged to further learn about and read technical field documents offered in the resources section.

Cross-References

- ▶ Emergency Management: Recent Incidents That Contributed to Changes in Emergency Management Legislation and Procedures
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Recovery
- ▶ Public-Private Partnerships: Training and Coordination in Disasters

References

Beeler, C. (2018). UN compact recognizes climate change as driver of migration for first time. Public Radio International. Retrieved from https://www.pri.org/stories/2018-12-11/un-compact-recognizes-climate-change-driver-migration-first-time.

Bullock, J. A., & Haddow, G. D. (2003). Introduction to Emergency Management. Burlington, MA: Butterworth-Heinemann.

Caribbean Hurricanes Fact Sheet #6. (2017 September 12). U.S.AID OFDA. Retrieved from https://www.usaid.gov/irma/fy17/fs6.

Centers for Disease Control (2017a). 2014 Ebola Outbreak in West Africa Epidemic Curves. Retrieved from https://www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/cumulative-cases-graphs.html.

Centers for Disease Control (2017b). 2014–2016 Ebola Outbreak in West Africa. Published December 27, 2017. Retrieved from https://www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/index.html.

Collins, A. E. (2018). Advancing the disaster and development paradigm. *International Journal of Disaster Risk Science, 9*, 486–495.

Coppola, D. P. (2015). *Introduction to international disaster management* (3rd ed.). Waltham: Elsevier.

Crescenzi, A., Ketzer, E., van Ommeren, M., Phuntsok, K., Komproe, I., & de Jong, J. T. V. M. (2002). Effect of political imprisonment and trauma history on recent Tibetan refugees in India. *Journal of Traumatic Stress, 15*(5), 369. https://doi-org.library.esc.edu/10.1023/A:1020129107279.

Dalal, A. (2017). Uncovering culture and identity in refugee camps. *Humanities, 6*, 61. https://doi.org/10.3390/h6030061. Retrieved from file:///C:/Users/Owner/Documents/Internat%20Disaster%20Management%202019%20chapt/uncovering%20culture%20and%20identity%20in%20refugee%20camps.pdf.

Disaster and Climate Change (2019). Norwegian Refugee Council. Retrieved from https://www.nrc.no/what-we-do/speaking-up-for-rights/climate-change/.

Dolma, S., Singh, S., Lohfeld, L., Orbinski, J. J., & Mills, E. J. (2006). Dangerous journey: Documenting the experience of Tibetan refugees. *American Journal of Public Health, 96*(11), 2061. https://doi-org.library.esc.edu/10.2105/AJPH.2005.067777.

Doshi, V. (2017). After nearly six decades of exile, some Tibetans in India are slowly letting go of the past. Published on October 9, 2017. Washington Post. Retrieved from https://www.washingtonpost.com/world/asia_pacific/after-nearly-six-decades-of-exile-some-tibetans-in-india-are-slowly-letting-go-of-the-past/2017/10/07/c00325b0-a2da-11e7-b573-8ec86cdfe1ed_story.html?utm_term=.d880123b8480.

Ferris, E. (2014). Too many humanitarian crises, not enough global resources. Brookings July 2014. Retrieved on 14 Mar 2019 from https://www.brookings.edu/opinions/too-many-humanitarian-crises-not-enough-global-resources/.

Fundamentals of Emergency Management. (2013). Chapter 13: International Emergency Management. Emergency Management Institute Federal Emergency Management Agency. Retrieved from https://training.fema.gov/hiedu/aemrc/booksdownload/fem/.

Gegout, C. (2015). 6 lessons from learned from the international response to Ebola. World Economic Forum. Retrieved from https://www.weforum.org/agenda/2015/02/6-lessons-from-the-international-response-to-ebola/.

Harmer, A., & Macrae, J. (2004). Beyond the continuum: The changing role of aid policy in protracted crises. Humanitarian Policy Group Research Report 18 July 2004. Retrieved on 14 Mar 2019 from https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/279.pdf.

Hess, J. M. (2009). Immigrant ambassadors: Citizenship and belonging in the Tibetan diaspora. Retrieved from https://ebookcentral.proquest.com.

International Organization on Migration (n.d.). Migration and climate change. Retrieved from https://www.iom.int/migration-and-climate-change-0.

Kannike, E. M. (2019). The ethnic and religious groups of Syria. Retrieved from https://syriancivilwarmap.com/ethnic-and-religious-groups-of-syria/.

Levy, B. S., & Patz, J. A. (2015). Climate change, human rights, and social justice. *Annals of Global Health, 81*(3), 310–322. https://doi.org/10.1016/j.aogh.2015.08.008.

Mahmood, J. (2015). Humanitarian funding is not enough: We must increase people's resilience. The Guardian 19 Jun 2015. Retrieved on 14 Mar 2019 from https://www.theguardian.com/global-development/2015/jun/19/humanitarian-assistance-funding-record-levels-increase-resilience.

Mattaini, M. A., & Lowery, C. T. (2007). Foundations of social work. In M. Mattani, C. Lowery, & C. Meyer (Eds.), *The foundations of social work practice: A graduate text* (4th ed.). Washington, D. C: NASW Press.

McKnight, J., & Plummer, J. M. (2015). Community Organizing: Theory and Practice. Pearson.

Medicines Sans Frontiers (2014). Project update. Retrieved from https://www.msf.org/international-response-west-africa-ebola-epidemic-dangerously-inadequate.

Miller, J. L. (2012). *Psychosocial capacity building in response to disasters*. New York: Columbia University Press.

Mincin, J. (2012). Strengths and weaknesses of the U.S.-based refugee resettlement program: A survey of International Rescue Committee Employee Perceptions. Doctoral dissertation. The City University of New York Graduate Center: NY.

Mincin, J., & Phillips, B. (2017). International and humanitarian disaster relief. In Phillips, B. (Eds), Introduction to Emergency Management, 2nd Ed. Boca Raton, FL: CRC Press.

Mincin, J. et al. (2013). Disability. In A. Fothergill, W. E. Lovekamp, B. Phillips, & D. S. K. Thomas (Eds), Social vulnerability to disasters, 2nd Ed. Boca Raton, FL: CRC Press.

Morse, I. for IRIN (2019). Ten humanitarian crises and trends to watch in 2019. Retrieved on 14 Mar 2019 from https://www.irinnews.org/feature/2019/01/02/ten-humanitarian-crises-and-trends-watch-2019.

Nickerson, G. L. (2018). Getting to the root of suffering: Dialogues with Tibetan refugee expolitical prisoners on what heals psychological and somatic sequelae of trauma. Dissertation Abstracts International: Section B: The Sciences and Engineering. ProQuest Information & Learning. Retrieved from http://library.esc.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2018-30618-128&site=eds-live.

OCHA Global Humanitarian Overview (2018). Retrieved on 14 Mar 2019 from https://interactive.unocha.org/publication/globalhumanitarianoverview/.

Parker, L. (2018). Retrieved from https://news.nationalgeographic.com/2018/03/climate-migrants-report-world-bank-spd/.

Philip, C. (2018). Fighting to feed the children left starving by a forgotten conflict; Yemen's civil war has put 22 million in need of humanitarian aid, Catherine Philp writes. The Times (London, England), [s. l.], 2018.

Phillips, B. D., Neal, D. M., & Webb, G. R. Eds (2017). Introduction to Emergency Management, 2nd Ed. Boca Raton, FL: CFC Press.

Ryan, D., Dooley, B., & Benson, C. (2008). Theoretical perspectives on post-migration adaptation and psychological well-being among refugees: Towards a resource-based model. *Journal of Refugee Studies, 21*(1), 1–18. Oxford, England: Oxford University Press.

Saleebey, D. (1999). *The strengths perspective: Principles and practices*. In B. R. Compton & B. Galaway. Social work processes (6th ed.). Pacific Grove, CA: Brooks/Cole. 14–23.

Saleeby, D. (1996). The strength perspective in social work practice: Extensions and cautions. *Social Work, 41*(3), 296–305.

Saxena, K. (2014). International response to Ebola crisis. Published by Institute for Defence Studies and Analyses. Retrieved from https://idsa.in/africatrends/international-response-to-ebola-crisis_ksaxena_0914.

Spilker, G., Koubi, V., Shaffer, L., & Böhmelt, T. (2018). There's grim news on climate change. Will it lead to mass migration and conflict? Washington Post online. October 15, 2018. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2018/10/12/how-does-climate-change-push-migration-and-conflict-heres-what-our-interviews-reveal/?utm_term=.857d2ce37235.

The Geneva Convention and Their Additional Protocols (n.d.). International Federation of Red Cross Red Crescent. Retrieved from https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions.

UNHCR (2018). UNHCR Turkey: Syrian refugee camps and provincial breakdown of syrian refugees registered in South East Turkey – 16 April 2018. Retrieved from https://data2.unhcr.org/en/documents/details/63246.

UNHCR (n.d.). UNHCR refugee coordination model. Retrieved from https://www.unhcr.org/excom/icm/53679e2c9/unhcr-refugee-coordination-model.html.

United Nations Commission on Human Rights Figures at a Glance (2018). Retrieved from https://www.unhcr.org/figures-at-a-glance.html.

United Nations Universal Declaration of Human Rights (n.d.). Universal Declaration of Human Rights (948). United Nations. Retrieved from https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217(III).

UNOCHA (n.d.). Who we are. Retrieved from https://www.unocha.org/about-us/who-we-are.

USAID (2018). Environment and global climate change. Retrieved from https://www.usaid.gov/what-we-do/environment-and-global-climate-change.

USAID (n.d.). Caribbean hurricanes. Retrieved from https://www.usaid.gov/irma.

What is the Cluster Approach? (n.d.). U.S. AID OFDA Humanitarian Response. Retrieved from https://www.humanitarianresponse.info/en/about-clusters/what-is-the-cluster-approach.

World Atlas (2018). How many countries are there in the world? Retrieved from https://www.worldatlas.com/articles/how-many-countries-are-in-the-world.html.

Wright, S., & Luisa, H. (2015). Wakeup call: Lessons from Ebola for the world health systems. Published by Save the Children, London. Retrieved from https://www.savethechildren.org.uk/content/dam/global/reports/health-and-nutrition/a-wake-up-call.pdf.

Further Reading

An Unspeakable Act. A Heroic Survivor – https://stories.usaid.gov/an-unspeakable-act-a-heroic-survivor/#page-1.

IASC Humanitarian System-Wide Scale-Up Activation: Definition and Procedures (2018). https://interagencystandingcommittee.org/iasc-transformative-agenda/content/iasc-protocol-1-humanitarian-system-wide-scale-activation.

IASC Strategy: Protection from and response to Sexual Exploitation and Abuse (SEA) and Sexual Harassment (SH) (2018). https://interagencystandingcommittee.org/iasc-senior-focal-points-sexual-exploitation-abuse-and-harassment/content/strategy-protection-and.

Sphere Handbook Humanitarian Chapter and Minimum Standards (2018). Retrieved from https://handbook.spherestandards.org/en/sphere/#ch001.

Thomas, D. S. K., Phillips, B. D., Lovekamp, W. E., & Fothergill, A. (2013). *Social vulnerability to disasters* (2nd ed.). London: CRC Press.
UN and IASC Cluster Approach. https://emergency.unhcr.org/entry/41814?lang=en_US.
UNHCR Emergency Handbook. https://emergency.unhcr.org/.
UNOCHA Global Humanitarian Overview. https://www.unocha.org/sites/unocha/files/publication/images/GHO2019_thumbnail.png.
UNOCHA Strategic Plan 2018–2012. https://www.unocha.org/sites/unocha/files/OCHA%202018-21%20Strategic%20Plan.pdf.

Emergency Management: Pets

Ashley K. Farmer[1] and Sarah E. DeYoung[2]
[1]Illinois State University, Normal, IL, USA
[2]University of Georgia, Athens, GA, USA

Keywords
Pets and disasters · Companion animals · Evacuation · Sheltering

Definition

The issue of emergency management and pets includes policies and research on how ownership of companion animals influences decisions in the context of disasters, including sheltering, evacuation, and re-entry considerations.

Introduction

Pet ownership affects the ways people react to and respond to disasters. These reactions include refusals to evacuate, early re-entry into closed areas to check on or retrieve pets, and psychological factors such as stress or trauma from the loss of a pet. Approximately 68% of Americans are pet owners (American Pet Products Association 2018), and therefore, the ways that pet ownership impacts evacuation and sheltering decisions during disasters remains a growing concern for emergency managers. Factors that influence the response of pet owners to disasters include attachment and commitment levels to pets, lack of proper evacuation plans, lack of available resources for transport and housing, and risk perception (Heath et al. 2001; Heath and Linnabary 2015). There are also complex issues related to the ways in which interest groups engage in decision-making to move and manage stray animals, wildlife, livestock, zoo, and research animals (Irvine 2009).

PETS Act

Pets are often considered a beloved part of families, and this is reflected not only in the passage of the PETS Act, but also in what is described as the sociozoologic scale (Arluke and Sanders 1996). This refers to the social categorization of some species as more or less deserving of attention and protection. Animals considered as pets have more value to humans, because there is often an emotional attachment and affection for the animal. With numerous images of pets left behind after Katrina, this bolstered support for the inclusion of animals in emergency management policies. After Hurricane Katrina in 2005, the issue of companion animals and disasters came to the forefront of public attention. This attention was a catalyst for the Pets Evacuation and Transportation Standards (PETS) Act (2006). Approximately 200,000 pets were abandoned or left behind during Hurricane Katrina, with just 5% of them ever reunited with owners (Lowe et al. 2009). The PETS Act requires that states include companion animals in disaster response plans in order to receive federal funding. Despite this, pet owners maintain primary responsibility for including their animals in household emergency plans. Additionally, shelters are not required to accept pets. The goal of this legislation was to provide additional resources to encourage evacuation compliance.

Evacuation and Sheltering

Households with pets are less likely to evacuate (Day 2017; Heath et al. 2001). Pets are often considered a part of the family, and many will refuse to leave if they cannot bring companion

animals along with them (Farmer et al. 2017; Leonard and Scammon 2007). In one study, respondents who owned pets were 52% more likely to choose to not evacuate (Petrolia and Bhattacharjee 2010). Weaker human-animal bonds have been associated with leaving pets behind, so the less attached one is to their pet the less likely it is they will evacuate their pets (Heath et al. 2001). Additionally, regular vet visits are associated with stronger attachment to companion animals. These pet owners are also more likely to include pets in disaster plans, suggesting that failure to evacuate with pets means there is a weaker bond and/or lower standard of care (Heath et al. 2001). One study found that low-income residents were more likely to leave animals behind during disaster events (Hesterberg et al. 2012), suggesting that access to resources is linked with ability to bring animals to the sheltering destination. Power structures and policies may also play a role in facilitating the evacuees' ability to bring their animals during an evacuation. For example, stories emerged after Hurricane Katrina that described owners who were forced to evacuate without their pets by first responders (Irvine 2009). Therefore, pet attachment and bonding are not the only factors in predicting the success of evacuation compliance.

Residents also might refuse to evacuate because they do not know where to take their pets, local shelters might not accept pets, or they cannot find information on pet-friendly shelters. Rumoring surrounding pets and proper evacuation protocols were evident during Hurricane Harvey and Irma (Federal Emergency Management Agency 2017). If leaving pets behind is not an option, residents will often stay behind with them if they cannot make other accommodations for animals. Pet owners who do evacuate are less likely to stay in a motel, hotel, or emergency shelter because those places lack pet accommodations or do not accept pets (Whitehead et al. 2000). A separate issue is that if residents evacuate quickly and leave pets behind, there is a possibility they will attempt to return early for their pets, which puts them in danger (Heath et al. 2001). This is more likely for a quick-onset disaster, where supplies are not readily prepared or available, and residents must leave immediately and do not have time to retrieve their pets.

Social Media and Reunification

There are also unexpected scenarios that might happen, including a pet becoming lost or running away during the evacuation or sheltering process, and they are separated from their owner. Reunification plans can become problematic if pets are not microchipped or do not have on identification tags. In the aftermath of recent hurricanes (e.g., Hurricanes Matthew, Harvey, and Irma), social media groups have been created with the aim of reuniting lost pets with owners (DeYoung and Farmer 2018). These groups have also publicized information about pet-friendly shelters, where individuals can go to volunteer help, and any animals that are in distress or need to be rescued.

Logistics and Planning

Other concerns have emerged about logistics of evacuating with companion animals (Farmer et al. 2017). Many supplies are needed for evacuating with pets, such as food, bowls, leashes, and carriers, and making sure there is room to bring pets. This can become a hassle for residents because traveling with pets is not an easy task. Additionally, they might be concerned about where to find pet friendly shelters or hotels. Those who do bring pets along might have to travel long distances to find accommodating hotels. Additionally, this can bring added stress for the animals themselves, as they are in unfamiliar locations and also dealing with the trauma of evacuation during a disaster. This can lead to some behavior changes in pets and ultimately create additional stressors or problems for their owners (DeYoung and Farmer 2018).

Conclusion

Emergency preparedness should continue to be integrated with pet ownership. This includes

helping individual households make emergency plans that include pets, widely disseminating information about pet friendly shelters, and state and local emergency managers effectively giving information to the public (Farmer et al. 2017). Companion animals are vulnerable during disasters because of their dependence on people (Bankoff 2014). Owning pets also increases risk for humans, since pet ownership has been linked to refusal to evacuate (Whitehead et al. 2000). Policies that continue to encourage emergency plans that include pets and state level planning for pet friendly shelters would ultimately increase evacuation compliance. Ultimately, the ownership of companion animals is connected to pre- and postdisaster decision-making processes.

Cross-References

- ▶ Emergency Management: Evacuations
- ▶ Emergency Management: Preparedness and Planning
- ▶ Natural Hazards

References

American Pet Products Manufacturers Association. (2018). *2017–2018 National pets owners survey.* Greenwich: American Pet Products Association.

Arluke, A., & Sanders, C. R. (1996). *Regarding animals*. Philadelphia: Temple University Press.

Bankoff, G. (2014). Learning about disasters from animals. In H. Egner, M. Schorch, & M. Voss (Eds.), *Learning and calamities: Practices, interpretations, patterns* (pp. 42–55). New York/London: Routledge.

Day, A. M. (2017). Companion animals and natural disasters: A systematic review of literature. *International Journal of Disaster Risk Reduction, 24*, 81–90.

DeYoung, S. E. & Farmer, A. K. (2018). Pets, Privilege, and Getting the Whole Story: Lessons Learned through Research on Companion Animal Evacuations for 2017 Disasters. Paper presented at Natural Hazards Workshop Researcher's Meeting, Broomfield, CO.

Farmer, A. K., DeYoung, S. E., & Wachtendorf, T. (2017). Pets and evacuation: An ongoing challenge in disasters. *Journal of Homeland Security and Emergency Management, 13*(4), 1–13.

Federal Emergency Management Agency. (2017). Rumor control for 2017. https://www.fema.gov/hurricane-irma-rumor-control

Heath, S. E., Kass, P. H., Beck, A. M., & Glickman, L. T. (2001). Human and pet-related risk factors for household evacuation failure during a natural disaster. *American Journal of Epidemiology, 153*(7), 659–665.

Heath, S. E., & Linnabary, R. D. (2015). Challenges of managing animals in disasters in the US. *Animals, 5*(2), 173–192.

Hesterberg, U. W., Huertas, G., & Appleby, M. C. (2012). Perceptions of pet owners in urban Latin America on protection of their animals during disasters. *Disaster Prevention and Management: An International Journal, 21*, 37–50.

Irvine, L. (2009). *Filling the ark: Animal welfare in disasters*. Philadelphia: Temple University Press.

Leonard, H. A., & Scammon, D. L. (2007). No pet left behind: Accommodating pets in emergency planning. *Journal of Public Policy & Marketing, 26*, 49–53.

Lowe, S. R., Rhodes, J. E., Zwiebach, L., & Chan, C. S. (2009). The impact of pet loss on the perceived social support and psychological distress of hurricane survivors. *Journal of Traumatic Stress, 22*, 244–247.

Petrolia, D. R., & Bhattacharjee, S. (2010). Why don't coastal residents choose to evacuate for hurricanes? *Coastal Management, 38*, 97–112.

Pets Evacuation and Transportation Standards (PETS) Act. (2006). Pub. L. No. 109-308, H.R. 3858, 109th Congress.

Whitehead, J. C., Edwards, B., Van Willigen, M., Maiolo, J. R., Wilson, K., & Smith, K. T. (2000). Heading for higher ground: Factors affecting real and hypothetical hurricane evacuation behavior. *Environmental Hazards, 2*, 133–142.

Further Reading

Edmonds, A. S., & Cutter, S. L. (2008). Planning for pet evacuations during disasters. *Journal of Homeland Security and Emergency Management, 5*(1), 1–18.

Potts, A., & Gadenne, D. (2014). *Animals in emergencies: Learning from the Christchurch earthquakes*. Christchurch: University of Canterbury.

Emergency Management: Preparedness and Planning

David A. McEntire
College of Health and Public Service, Utah Valley University, Orem, UT, USA

Keywords

Capacity building · Emergency operation plan · Preparedness · Planning

Definition

Preparedness is a broad, encompassing concept in emergency management that "involves anticipatory measures taken to increase response and recovery capabilities" (McEntire and Myers 2004, p. 141). A component of preparedness in emergency management is planning, which is defined as the "logical and analytical problem-solving process to help address the complexity and uncertainty inherent in potential hazards and threats" (FEMA 2010, pp. 1–3).

Introduction

Preparedness and planning in daily life imply getting ready for something of significance that is anticipated to take place or occur in the future. In emergency management and homeland security, preparedness and planning have a similar connotation, but mainly deal with efforts to help individuals, organizations, communities, and even the nation to anticipate and cope with emergencies, terrorist attacks, and disasters (see ▶ "Emergency Management: Crisis Management and Response" in this encyclopedia). In this sense, preparedness and planning are concepts and activities that are often closely related and convoluted, but they are not always or entirely synonymous.

Preparedness is a broader, more encompassing concept that is comparable to other phases/functions of emergency management (e.g., mitigation, response, and recovery) as well as the phases/functions of homeland security (e.g., prevention and protection). For instance, mitigation and preparedness occur before a disaster like prevention and protection, although mitigation is concerned about the reduction of risk and impacts, whereas preparedness assumes disasters and attacks will occur. In addition, preparedness is related to response and recovery since it is believed to improve operations in the aftermath of all types of emergencies, terrorist attacks, and disasters (see ▶ "Emergency Management: Crisis Management and Response" in this encyclopedia).

In contrast to preparedness, the term planning is often considered a subset or very specific type of action under the function of preparedness. As an example, planning includes a projection of what disasters may occur and a description of what should be done to react to such hazards, threats, and vulnerabilities. Thus, both preparedness and planning capture efforts to improve readiness to deal with emergencies, disasters, terrorist attacks, and their specific consequences. The nature of preparedness and planning will be discussed further with specific examples of each type of activity.

Understanding Preparedness

Views about preparedness vary slightly among emergency management and homeland security institutions/practitioners and the scholars who study disasters. And, this concept is not always used consistently within organizations or by individuals. For instance, the Federal Emergency Management Agency (FEMA. 2019a) defines preparedness as a "continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response" (p. 1). However, FEMA (2015) also purports that preparedness is an overarching effort that captures all aspects of emergency management and homeland security. As an example, in its National Preparedness Goal, FEMA notes the priority of developing "a secure and resilient national with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" (FEMA 2015, p. 1).

FEMA has likewise created a National Preparedness System that entails six major priorities: identifying and assessing risk, estimating capability requirements, building and sustaining capabilities, planning to deliver capabilities, validating capabilities, and reviewing and updating (FEMA 2019b). These priorities have the goal of helping the nation anticipate disasters and effectively respond when they occur. Examples of each priority are mentioned below.

Priorities	Example
Identifying and assessing risk	Determining if an earthquake could occur and what the impacts will be
Estimating capability requirements	Making educated guesses about the need for rescue operations, fire suppression, and emergency medical care
Building and sustaining capabilities	Purchasing fire apparatus, extraction equipment, and medical supplies
Planning to deliver capabilities	Training with apparatus, equipment, and supplies
Validating capabilities	Completing a disaster exercise
Reviewing and updating	Learning from exercise and replacing old equipment

In addition to the 6 major priorities, FEMA has identified 32 core capabilities in its National Preparedness Goal (2019c). While the priorities are meant to improve preparedness processes, these core capabilities suggest ways to improve the performance of typical functions in a disaster. They include:

- Planning
- Public information and warning
- Operational coordination
- Forensics and attribution
- Intelligence and information sharing
- Interdiction and disruption
- Screening, search, and detection
- Access control and identity verification
- Cybersecurity
- Physical protective measures
- Risk management for protection programs and activities
- Supply chain integrity and security
- Community resilience
- Long-term vulnerability reduction
- Risk and disaster resilience assessment
- Threats and hazards identification
- Critical transportation
- Environmental response/health safety
- Fatality management services

As can be seen, FEMA's view of preparedness is extensive and closely tied to terrorism and homeland security since it concentrates on activities such as forensics, intelligence, interdiction, screening, access control, cybersecurity, protective measures, etc. FEMA also suggests that preparedness is what a community, state, or nation does to build capacity to address all types of emergency management/homeland security functions. Capacity building implies "an ongoing process that equips officials, stakeholders and the community to perform their functions in a better manner during a crisis/disaster" (NDMA 2019).

Like their counterparts in emergency management and homeland security, professors and researchers also see preparedness as a foundational principle in these important areas (Kreps 1991, p. 31). However, scholars are more likely to consider preparedness in a slightly narrower fashion than does FEMA, mainly concentrating on what is done in advance of a disaster to get the community ready to react in an effective and efficient manner. For instance, Godschalk (1991) views preparedness as "actions taken in advance of an emergency to develop operational capabilities and to facilitate an effective response in the event an emergency occurs" (p. 136). McEntire and Myers (2004) assert that preparedness "involves anticipatory measures taken to increase response and recovery capabilities" (p. 141).

Under this academic perspective, mitigation does not generally fall under the concept of preparedness. Instead, mitigation is concerned more about disaster prevention, while preparedness is more focused on readiness for disasters. Therefore, scholars believe mitigation and preparedness have different assumptions (e.g., mitigation assumes disaster prevention or reduction is possible, while preparedness assumes a disaster will occur and that response and recovery will therefore be necessary).

Although FEMA and scholars view preparedness differently, there are still considerable similarities between the professionals and scholars who are involved with disasters, emergency management, and homeland security. Both groups view preparedness as a major priority to successfully anticipate contingencies and make improvements on how best to react to them.

Specific Preparedness Activities

Preparedness in emergency management and homeland security is multifaceted and quite complex. For example, Mileti (1991) stated that "the purpose of preparedness is to anticipate problems in disasters so that ways can be devised to address the problems effectively and so that the resources needed for an effective response are in place before-hand" (p. 215). He further elaborated that "preparedness includes such activities as formulating, testing, and exercising disaster plans; providing training for disaster responders and the general public; and communicating with the public and others about disaster vulnerability and what to do to reduce it" (p. 215).

In similar fashion, Gillespie and Streeter (1987, p. 155) asserted that preparedness includes planning, resource identification, the development of warning systems, training and simulations, and other pre-disaster actions taken for the sole intent of improving the safety and effectiveness of a community's response during a disaster. Preparedness therefore includes a plethora of activities, which may also include:

- Legislative mandates and organizational creation (e.g., the establishment of laws pertaining to disasters and terrorist attacks)
- Resource identification, budget acquisition, and grant management (e.g., obtaining equipment and personnel and allocating and spending funds to reach emergency management and homeland security goals)
- Risk assessment (e.g., identifying anticipated hazards, threats, and vulnerabilities)
- Planning (which will be discussed further below)
- Organizational structures that facilitate operations (e.g., establishing an emergency operations center, an incident command structure, and mutual aid agreements)
- Warning system development (e.g., establishing policy and acquiring technology to notify people in advance or provide updates as needed after the event)
- Training (e.g., teaching employees in official capacities about the plan and their role in emergency management and homeland security)
- Exercising (e.g., determining the level of understanding of the plan and ability to fulfill required tasks)
- Community education (e.g., ensuring that the public understands what can be done in advance of a disaster or terrorist attack and how they should react if such events occur)

Because there are so many features of preparedness, it is often difficult to know the true state of readiness. A city may have exceptionally detailed ordinances, but neglect to adequately fund the emergency management organization. An emergency manager may focus heavily on risk assessment, but fail to develop or adequately update comprehensive disaster plans. A fire department may spend considerable time training fire fighters on fire suppression, but not give enough attention to public education about the importance of the installation of smoke detectors in residential or commercial buildings. A community may be ready to deal with a hurricane, but could be less capable of dealing with a pandemic or terrorist attack. For this reason, preparedness is likely to be incomplete and must be seen as an ongoing process rather than a simple checklist to be completed.

Understanding Planning

Disaster planning is not interpreted or understood in the same way for different people and organizations, and like preparedness, there is no single agreed-upon definition. Nevertheless, disaster planning is often related to the creation of "systematic procedures that clearly detail what needs to be done, how, when, and by whom before . . . an anticipated disastrous event occurs" (Businessdictionary.com 2019, para 1). Relevant to this discussion is the Emergency Operations Plan (EOP), "a document that describes how the jurisdiction might respond to a disaster" (McEntire 2015, p. 131).

As noted above, planning is one of several different aspects of preparedness – although it should be pointed out that planning is one of the most well-known and essential elements of preparing for all types of disasters and terrorist attacks.

There are several key principles associated with this important concept:

1. Planning entails an identification of what types of emergencies, disasters, and terrorist attacks may occur. This may include natural, technological, and civil hazards of all categories and scope.
2. Planning also includes an anticipation of the consequences of such events. The impacts may vary from injuries, death, property destruction, and social disruption.
3. Planning involves all key participants and clarifies what will be done and who will do it. The goal is to specify who is responsible for each area or activity and how individuals and agencies will coordinate with others.
4. Planning almost always refers to the creation of a written document that describes what the organization or community will do in the case of an emergency, terrorist attack, or disaster. This document is known as an Emergency Operations Plan (EOP). It is typically made up of the basic plan (a general overview), annexes (which can be hazard-specific or functional), and appendices (such as supporting documents, standard operating procedures, maps, resource lists, etc.).
5. Planning must be based on accurate assumptions (Dynes 1994). It is important to understand how people will react in disasters, rather than assume incorrect behaviors and create plans with mistaken expectations.
6. Planning should never be considered complete or a silver bullet. Auf der Heide warns against the "paper plan syndrome" by explaining that "written plans indeed are very important, but they are only one of the necessary requirements . . . . A written plan can be an illusion of preparedness if the other requirements are neglected" (1989, p. 34).

Despite these key principles, planning may take different forms. While there is no universal standard for disaster planning, most EOPs do contain various sections including descriptions about authority, purpose, situation and assumptions, concept of operations, organization and assignment of responsibility, direction and control, plan development/maintenance, and implementation. FEMA (2010) has also provided several recommendations for communities in its Comprehensive Planning Guide 101. This document "provides methods for planners to:

- Conduct community-based planning that engages the whole community by using a planning process that represents the actual population in the community and involves community leaders and the private sector in the planning process.
- Ensure plans are development through an analysis of risk.
- Identify operational assumptions and resource demands.
- Prioritize plans and planning efforts to support their seamless transition from development to execution for any threat or hazard.
- Integrate and synchronize efforts across all levels of government" (FEMA 2010, i).

CPG 101 therefore provides recommendations on the basics of planning, the context of planning (e.g., federal, state, and local environment), the format of plans, the planning process, etc. It is a useful guide to help emergency managers meet federal planning expectations.

Specific Planning Activities

The activities subsumed under the label of planning are almost endless. However, there are four main themes prevalent in the literature. First, planning focuses on different types of disasters (e.g., earthquakes, hurricanes, flooding, tornadoes, dam failures, fires, climate change, pandemics, nuclear accidents, chemical spills, terrorist attacks, etc.). Second, planning concentrates on diverse functions that must be performed during or after a disaster (e.g., hazard detection, warning, evacuation, sheltering, search and rescue, triage and medical care, mass fatality management, stress management/mental health, public information/social media, donations management, volunteer management, damage assessment, disaster declarations, debris

management, disaster assistance, communications and coordination, decision-making, transportation and logistics, organizational continuity, rebuilding, etc.). Third, planning identifies the needs of special individuals and groups (e.g., gender, race, poor, tourists, the elderly/nursing home residents, children, the disabled, hospital patients, tribal communities, animals, etc.). Finally, planning gives attention to unique situations or locations (e.g., civil disturbances, parades, major sporting events like the Super Bowl, a Presidential inauguration, day care centers, libraries, museums, airports, hospitals, schools/universities, the workplace, water/waste water facilities, power plants, farms/food processing plants, government buildings/courts, small cities/large cities, rural communities/urban communities, etc.).

As noted, the important priority of planning is to make sure the community is considering all types of eventualities and that its pre-disaster efforts do not end with the creation of an Emergency Operations Plan (EOP) but rather pursue the goal of building capabilities. As noted earlier, building capabilities may be defined as creating the ability to successfully implement the plan. This is important since planning is incomplete in and of itself. As an example, the city of New Orleans had a very comprehensive Emergency Operations Plan prior to Hurricane Katrina which clearly detailed the potential for a hurricane and flooding, the need for evacuation and sheltering, and how to care for anticipated victims. Unfortunately, the jurisdiction was unable to implement the plan effectively (e.g., evacuate citizens by school bus, provide enough resources at the Superdome, etc.). Government leaders in New Orleans had a very detailed EOP, but unfortunately lacked the ability to implement the plan.

The Benefit of Preparedness and Planning

Virtually everyone agrees that preparedness and planning have a positive impact on response and recovery operations. Effective preparedness and planning may:

- Identify resources for response and recovery (Auf der Heide 1989, p. 39)
- Improve personal relationships among those working in emergency management (Dynes 1994, p. 147)
- Increase interorganizational coordination (Auf der Heide 1989, p. 39)
- Facilitate improvisations (Kreps 1991, p. 34)
- "Help save lives, reduce injuries, limit property damage, and minimize all sort of disruptions that disasters cause" (Mileti 1991, p. 239)

Consequently, preparedness and planning are some of the most important aspects of emergency management and homeland security (McEntire 2015).

Conclusion: Future Preparedness and Planning Needs

Preparedness and planning are vital components of emergency management and homeland security. Both deal with efforts to increase readiness for disasters and terrorist attacks. However, preparedness is a broader concept that covers many actions, while planning is one specific type of preparedness initiative that often focuses on developing an Emergency Operations Plan.

While much is known about preparedness and planning, more research is required. In spite of thousands of citations in the literature, there is still insufficient agreement on the best way to promote these key principles in emergency management and homeland security. For instance, what can be done to help communities prepare for disasters when these events are considered to be unlikely or viewed as being beyond human efforts of intervention? Are certain planning templates and processes more effective than others? Which ones and why? (See ▶ "Emergency Management: Best Practices" in this encyclopedia.) Not enough is known about what constitutes an effective plan, and there is insufficient empirical research (as opposed to anecdotal studies) on this subject.

Furthermore, additional emphasis on preparedness should be given in order to increase response and recovery capabilities of individuals, organizations, and governments. Too often people and institutions assume they are prepared because they have

a plan (i.e., the paper plan syndrome). Finally, more education and training on planning are also necessary. Emergency managers do have knowledge about planning, but their level of expertise could be expanded and deepened.

Cross-References

- ▶ Emergency Management: Best Practices
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Recovery
- ▶ Terrorism: Homegrown

References

Auf der Heide, E. (1989). *Disaster response: Principles and preparation for coordination*. St. Louis: C.V. Mosby Company.

Business Dictionary.com. (2019). "Disaster plan." www.businessdictionary.com/definition/disaster-plan.html. Access 18 July 2019.

Dynes, R. R. (1994). Community emergency planning: False and inappropriate analogies. *International Journal of Mass Emergencies and Disasters, 12*(2), 141–158.

FEMA. (2010). *Developing and maintaining emergency operations plans: Comprehensive preparedness guide 101*. Version 2.0 (November). https://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparedness_guide_developing_and_maintaining_emergency_operations_plans_2010.pdf. Accessed 24 July 2019.

FEMA. (2015). "National preparedness goal." https://www.fema.gov/media-library.data/1443799615171-2ae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf. Accessed 25 July 2019.

FEMA. (2019a). "Plan and prepare for disasters." https://www.dhs.gov/plan-and-prepare-disasters. Accessed 25 July 2019.

FEMA. (2019b). "National preparedness system." https://www.fema.gov/national-preparedness-system. Accessed 23 July 2019.

FEMA. (2019c). "Core capabilities." https://www.fema.gov/core-capabilities. Accessed 25 July 2019.

Gillespie, D. F., & Streeter, C. L. (1987). Conceptualizing and measuring disaster preparedness. *International Journal of Mass Emergencies and Disasters, 5*(2), 155–176.

Godschalk, D. R. (1991). Disaster mitigation and hazard management. In T. Drabek & G. Hoetmer (Eds.), *Emergency management: Principles and practices for local government* (pp. 131–160). Washington, D.C.: International City Management Associate.

Kreps, G. A. (1991). Organizing for emergency management. In T. Drabek & G. Hoetmer (Eds.), *Emergency management: Principles and practices for local government* (pp. 30–54). Washington, D.C.: International City Management Associate.

McEntire, D. A. (2015). *Disaster response and recovery: Strategies and tactics for resilience*. Hoboken: Wiley.

McEntire, D. A., & Myers, A. (2004). Preparing communities for disasters: Issues and processes for government readiness. *Disaster Prevention and Management, 13*(2), 140–152.

Mileti, D. S. (1991). *Disasters by design: A reassessment of natural hazards in the United States*. Washington, D.C.: Joseph Henry Press.

NDMA. (2019). *Capacity building*. National Disaster Management Authority: India. https://ndma.gov.in/en/about-ndma/divisions/administration/cbt.html. Accessed 23 July 2019.

Further Reading

Alexander, D. E. (2015). Disaster and emergency planning for preparedness, response and recovery. In *Oxford research encyclopedia of natural hazard science* (pp. 1–20). Oxford: Oxford University Press.

Coppola, D. P., & Maloney, E. K. (2017). *Communicating emergency preparedness: Practical strategies for the public and private sectors*. Boca Raton: CRC Press.

Schwab, A. K., Brower, D. J., & Sandler, D. (2016). *Hazard mitigation and preparedness: An introductory text for emergency management and planning professionals*. Boca Raton: CRC Press.

Emergency Management: Recent Incidents That Contributed to Changes in Emergency Management Legislation and Procedures

Anna Stamper
Homeland Security, Disaster and Emergency Management, Eastern Kentucky University, Richmond, KY, USA

Keywords

Emergency management · Preparedness · Response · Mitigate · Legislature

Definition

Emergency management is the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters. Particularly, emergency management encompasses preparedness, planning, response, recovery, and mitigation of hazards and threats.

Introduction

Emergency management organizations protect communities by coordinating and integrating all activities necessary to build, sustain, and improve the capability to mitigate against, prepare for, respond to, and recover from threatened or actual natural disasters, acts of terrorism, or other man-made disasters. These organizations offer a wide array of services that enable them to handle a broad range of negative events (i.e., hazards and disasters). The Federal Emergency Management Agency (FEMA 2018), under the auspices of the Department of Homeland Security since 2003, functions as our nation's emergency manager to train our first responders to be prepared and provide security, handle a variety of hazards and threats, and help communities "before, during, and after disasters" (see entry entitled ▶ "Federal Emergency Management Agency" in this encyclopedia).

This entry focuses on the legislative (e.g., laws, acts, policies) and procedural impact of six events based on aftermath reports to improve all phases – planning, preparedness, recovery, and responses – of emergency management. Aftermath reports have been the main source for determining the strengths and weaknesses of the current emergency plans on a community's citizen health, psychological well-being, and resilience. This entry focuses on six events discussed in historical order – September 11 (2001), Hurricane Katrina (2006), Department of Defense Cyber Attacks (2008), Deepwater Horizon Oil Spill (2010), Hurricane Sandy (2012), and Oso Landslide (2014).

September 11 Terrorist Attacks

The terrorist attacks that took place in New York, Pennsylvania, and Washington D.C. on September 11, 2001, led to changes in both legislation and procedure. First, the Homeland Security Act of 2002 (see entry in ▶ "Homeland Security Act of 2002") was created to protect the nation from terrorism. Second, the Federal Emergency Management Agency (FEMA) initiated a Federal Response Plan (Public Law 93-288) to coordinate natural disasters (e.g., hurricanes, floods, fires) and technological emergency situations (e.g., radiological or hazardous materials) by mobilizing resources and augment response efforts. Third, FEMA (2004) provided its recommendations for coordinating emergency and disaster procedures by first responders under National Incident Management System (NIMS).

Subsequently, the 9/11 Commission Act (2007) addressed a wide range of DHS's missions, including critical infrastructure protection, grant administration, intelligence and information sharing, privacy, and transportation security, including aviation and bus transportation. The Act led to amendments in Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), expanded and refined the scope of the Information Sharing Environment (ISE) of the Homeland Security Act of 2002, and established guidelines for fusion centers (Homeland Security Digital Library 2017). This Act also determined fair distribution of Homeland Security grants, with over 90% of these grants allocated on a risk-based basis; required screening of ALL cargo that was being transported by passenger airplanes with limited exceptions; allotted $4 billion in grants to upgrade and implement security measures in rail, transit, and buses; and provided lawful protection of citizens who, in good faith, reported alleged or suspected terrorist activity on buses, trains, or airplanes.

Hurricane Katrina (2006)

Although Hurricane Katrina occurred in 2006, this devastating natural disaster left lasting effects

and changes in the field. This disaster most notably tested the performance of the Federal Emergency Management Agency (FEMA), which was integrated into the Department of Homeland Security (DHS) in 2003, just 3 years prior. At the time, Hurricane Katrina was the most significant disaster that FEMA faced since being absorbed by DHS. From the moment that Hurricane Katrina was determined to be a major threat to, specifically, the Gulf Coast and the City of New Orleans, there were issues and incompetence in both the federal agencies and the local responders regarding communication, planning, evacuation, and sheltering arose. As a whole, the effects and shortcomings that were seen during Hurricane Katrina helped FEMA and DHS to identify and address these shortcomings to better prepare for future disasters and events.

Hurricane Katrina had a significant impact on legislation through the development of the PETS Act of 2006, the Katrina Emergency Assistance Act, and Public Law 109-295. The Pets Evacuation and Transportation Standards (PETS) Act of 2006 amended the Robert T. Stafford Disaster Relief and Emergency Assistance Act ("The Stafford Act") to require the Director of FEMA to ensure that state and local emergency preparedness operational plans address the needs of individuals with household pets or service animals prior to, during, and following a major disaster or emergency.

The Katrina Emergency Assistance Act of 2006 also directed the President to make unemployment assistance available to individuals eligible for such assistance under the Stafford Act as a result of a disaster declaration made for Hurricanes Katrina or Rita on or after August 29, 2005, and for 39 weeks after the declaration date. This act was particularly impactful because the basis of this act has been adopted and specifically adapted for nearly every major disaster since Hurricane Katrina, to ensure that victims of disasters receive assistance required after a major disaster.

Public Law 109-295 of the Department of Homeland Security Appropriations Act of 2007 is the Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA). This act "provided important provisions, including the key principle that after a major disaster or emergency declaration accelerated Federal assistance could be sent by FEMA, in the absence of a specific request by a State, to save lives and prevent suffering." Essentially, this act helped shortcomings that were brought to attention by Hurricane Katrina. The PKEMRA also established the following: Disability Coordinator; the National Emergency Family Registry and Locator System; better evacuation processes and recovery efforts following major disasters; improved transportation assistance for evacuation efforts and returning individuals to their homes following a major disaster; and case management assistance for survivors who claim unmet needs after a disaster.

2008 Department of Defense Cyber Attacks

In 2008, an infected flash drive was inserted into a military laptop from a base in the Middle East and launched the most impactful cyberattack that the US military had ever encountered. The overall goal of the attack was to infiltrate the classified systems and files on the laptop and remotely relay the information back to the owner of the flash drive, who was unknown at the time. While this particular cyberattack on the US military and its defense systems was unsuccessful, it reversed many instabilities in the United States and the military's cyber security and response efforts.

As a result of this attack, the Pentagon updated their layered defense networks built around military and high-profile networks, all of which were at risk. Additionally, the United States Cyber Command was implemented. According to a 2013 fact sheet published by the US Cyber Command's Public Affairs Office, the United States Cyber Command "plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the

same to our adversaries." The United States Cyber Command is tasked with centralizing command of cyberspace operations, strengthening DoD cyberspace capabilities, and integrating and bolstering DoD's cyber expertise. This particular attack also began discussions between the US military, federal government, and other agencies about what the widespread response and plan was in the event of a cyberattack in any sector of the military, government, or other agencies.

While there were many preventative defense procedures and mitigation techniques that stemmed from this attack, there were few legislative acts passed and implemented as a result. Most legislation has occurred within specific governmental organizations, with new rules and policies implemented agency-wide in various agencies in order to prevent another attack of this kind and caliber from occurring again in the United States. Additionally, there have been various legislatures passed as a result of the formation of the United States Cyber Command; however, there is no direct, stated influence from the 2008 cyberattacks for this legislature.

Deepwater Horizon Oil Spill (2010)

On April 20, 2010, the oil drilling rig "Deepwater Horizon," operating in the Macondo Prospect in the Gulf of Mexico, exploded and sank resulting in the death of 11 workers on the Deepwater Horizon and the largest spill of oil in the history of marine oil drilling operations. The Deepwater Horizon Oil Spill was one of the first major environmental disasters that the United States had ever faced and was one of the most environmentally damaging. In addition to the 11 deaths as a result of this disaster, wildlife and marine life were damaged by the four million barrels of oil that flowed into the ocean over an 87-day period.

In the moments after the initial explosion which caused the dispersion of the vast amounts of oil, communications between British Petroleum (BP), the company responsible for the spill, the National Oceanic and Atmospheric Administration (NOAA), and emergency responders were extremely weak and ultimately hindered rescue, cleanup, and recovery efforts. This resulted in a reform of communication strategies between private companies, national and federal agencies, and programs, in the event of a similar emergency or disaster in the future. Additionally, this event also identified weak points in the recovery efforts of environmental disasters which are far less likely to occur than naturally occurring disasters. Because limited information exists on oceanic oil spills or their effects on ecosystems and wildlife, human health, and the economy, emergency management agencies were made aware that more thorough incident training for emergencies that are extremely unlikely but highly dangerous events must be integrated into current plans and procedures, for both preparation and response.

Because of its massive impact on the oil drilling industry, local wildlife and oceans, and the threat of another similar event occurring, the Deepwater Horizon Oil Spill led to the passing and implementation of many drilling regulations in the United States. In addition to these regulations, which helped ensure the safety and security of drilling sites and rigs, multiple agencies were formed as a direct result of the Deepwater Horizon Oil Spill. While there were many regulations and agencies formed and implemented as a result of this disaster, there are a lack of publications regarding laws and legislature passed as a direct result of this event.

The Bureau of Safety and Environment Enforcement (BSEE) was established by Secretarial Order 3299 as a direct response to the failures of the Minerals Management Service (MSS) in response to the Deepwater Horizon Oil Spill. Order 3299 also created the Bureau of Ocean Energy Management (BOEM) and the Office of Natural Resources Revenue (ONRR), all integrated into the Department of the Interior. The missions of these three entities are to ensure the balance and responsible development of energy resources on the outer continental shelf, where offshore drilling and other potentially harmful activities occur; ensure safe and environmentally responsible exploration and production while enforcing applicable rules and regulations; and ensure a fair return to the taxpayer from offshore royalty and revenue collection and disbursement activities.

Hurricane Sandy (2012)

Hurricane Sandy, which occurred from October 22, 2012, to November 2, 2012, was the largest Atlantic hurricane on record and severely impacted the states of New Jersey and New York. Damage caused as a direct result of this disaster was vast. Seventy-one people died from the hurricane, while a total of $65 million in damages. As the fourth costliest hurricane in the history of the United States, Hurricane Sandy tested FEMA and other agencies tasked with emergency management, preparedness, and management responsibilities, many of which had dealt with the fallout of Hurricane Katrina as well. Their role in Hurricane Katrina gave many agencies the insight and information needed in order to deal with many aspects of this hurricane differently than Katrina was handled.

Regarding legislation, two major bills passed in the wake of Hurricane Sandy – the Disaster Relief Appropriations Act (2013) and the Hurricane Sandy Relief Bill. The Disaster Relief Appropriations Act authorized a grant of $60 billion to be distributed to 21 different disaster relief agencies, including FEMA, the Department of Homeland Security, and the Army Corps of Engineers. The Hurricane Sandy Relief Bill amended the National Flood Insurance Act of 1968 to increase the total federal borrowing authority for the National Flood Insurance Program from $20.725 billion to $30.425 billion (a $9.7 billion difference).

Oso Landslide (2014)

A large landslide occurred in northwest Washington state on March 22, 2014, leading to tragic loss of life and destruction of property. Landslide debris covered approximately 40 homes and other structures as well as nearly a mile of State Route 530. It also caused 43 fatalities in the community of Steelhead Haven near Oso, Washington. The main impact that the Oso Landslide had on emergency management was the importance of communication and transparency between government officials, private industry, and citizens. In the years leading to the Oso landslide, it was reported that government officials knew that extensive logging in the Oso area was diminishing the structural integrity of the mountains in Oso and the public was not informed. Many citizens lived in the high-risk zone for landslides in the area, but they were never made aware until after the landslide occurred. Because of this, communication and transparency between government officials and citizens have been at the forefront for planning and emergency management efforts to date.

Because of the sheer disregard of warning signs and public communication by local and government officials that took place in regard to the Oso Landslide, the National Landslide Preparedness Act was introduced and implemented in 2017 and is currently waiting amendment. By enacting this bill, a new step toward preparedness will be taken to ensure protection of life and property in an event comparable to the Oso Landslide. The National Landslide Preparedness Act directs the US Geological Survey (USGS) to establish a National Landslide Hazards Reduction Program to identify and understand landslide hazards and risks, reduce losses from landslides, protect communities at risk of landslide hazards, and improve communication and emergency preparedness and establishes the Interagency Coordinating Committee on Landslide Hazards to oversee the program.

With advancements in technology, concomitant improvements have occurred in the way that geologists and scientists are able to predict events that would exist in such a scale, as the Oso Landslide did. There have also been major policy overhauls in areas that are known to have the same geographical makeup as Steelhead Haven and are at risk for similar types of events.

Conclusion

While every highlighted event in this entry varied from the type of event to the severity, every event helped emergency management agencies

understand the improvements that needed to be made to legislation, response, recovery, and preparedness. Many events, such as Hurricane Katrina and the Oso Landslide, caused a reaction from legislators, which sparked an increase in disaster preparedness and response and emergency management legislature. Other events, such as the 2009 Department of Defense Cyber Attacks and the Deepwater Horizon Oil Spill, ushered in new conversations about potentially targeted areas, such as cyberspace and the natural environment. Every event highlighted in this entry helped initiate a change for emergency management and response legislature and increased communication about how it can be improved. The changes that have been made as a result of these events have been successful and positive, and the future of successful emergency management lies in the ability to understand the changes that need to be made and change them.

Cross-References

- ▶ Emergency Management: Best Practices
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Preparedness and Planning
- ▶ Emergency Management: Recovery

References

Federal Emergency Management Agency. (2004). FEMA releases recommendations for emergency response to major incidents based in part on the events of Sept. 11, 2001. Accessed at: https://www.fema.gov/news-release/2004/05/26/fema-releases-recommendations-emergency-response-major-incidents-based-part. 6 Nov 2019.

FEMA Outlines a Decade of Progress after Hurricane Katrina. (2018). Retrieved from https://www.fema.gov/news-release/2015/07/30/fema-outlines-decade-progress-after-hurricane-katrina

Homeland Security Digital Library (2017). A legal and policy approach for responsible information sharing. Accessed at: https://www.hsdl.org/?view&did=720070 (7/21/2020)

Further Reading

9-11 Commission, Homeland Security, and Intelligence Reform. (n.d.). Retrieved from https://www.hsgac.senate.gov/issues/9-11-commission

Cyberattack in 2008 prompted new Pentagon cyberdefense plan. (2010, August 25). Retrieved from http://www.cnn.com/2010/TECH/innovation/08/25/pentagon.cyberattack/index.html

Hurricane Sandy Fast Facts. (2017, October 19). Retrieved from https://www.cnn.com/2013/07/13/world/americas/hurricane-sandy-fast-facts/index.html

Kamien, D. (2012). *The McGraw-Hill homeland security handbook: Strategic guidance for a coordinated approach to effective security and emergency management* (2nd ed.). New York: McGraw-Hill.

One Year Later – The Oso Landslide in Washington. (n.d.). Retrieved from https://www.usgs.gov/news/one-year-later-–-oso-landslide-washington

Pallardy, R. (2018, April 13). Deepwater Horizon oil spill of 2010. Retrieved from https://www.britannica.com/event/Deepwater-Horizon-oil-spill-of-2010

Post-Katrina Emergency Management Reform Act of 2006. (n.d.). Retrieved from https://www.hsdl.org/c/tl/post-katrina-emergency-management-reform-act-2006/

Rubin, C. B. (2012). *Emergency management: The American experience 1900–2010* (2nd ed.). Boca Raton: CRC Press.

U.S. Cyber Command Public Affairs. U.S. Cyber Command fact sheet. U.S. Cyber Command – U.S. Strategic Command. https://web.archive.org/web/20140416192156/http://www.stratcom.mil/factsheets/2/Cyber_Command/

Emergency Management: Recovery

Paolo Cavaliere
University of Delaware, Newark, DE, USA

Keywords
Emergency management · Recovery · Business recovery · Housing

Definition

Disaster recovery is the set of coordinated activities through which public agencies, nonprofit organizations, private sector, and communities work together in order to rebuild and restore

normal conditions after disasters. Recovery strategies encompass practices and actions that aim to restore the social, infrastructural, and economic fabric of communities.

Introduction

During the last decade, humanity has witnessed an increased number of deadly events. Only for weather-related events, NOAA reports a number of 108 events with an economic impact of $725 billion. (Billion-Dollar Weather and Climate Disasters: Summary Stats. https://www.ncdc.noaa.gov/billions/summary-stats.) Tropical cyclones account for a 56% of the overall loss. Besides the American situation, the impact on communities and the overall economic costs after disasters is a burden that governments attempt to lighten, adopting mitigation measures that should be more effective when the next big disaster occurs. Unfortunately, not always the mitigation strategies prove effective; the level of preparedness might not be enough for coping with disasters. Therefore, governments, at any level, are overwhelmed with response operations. Once response operations are considered "over," agencies start working on recovery. The emergency management framework consists of four specific phases: mitigation, preparedness, response, and recovery. During the mitigation phase, emergency managers, planners, and experts look at long-term solutions that aim to reduce the impact of hazards on infrastructures, lifelines, essential services, and communities; mitigation measures apply to the natural and the built environment. While mitigation aims to reduce the impact of hazards, preparedness instead focuses on how ready systems and communities are to respond to adverse events. Preparedness presumes an integrated set of activities that allow agencies and emergency services to be always efficient with sufficient resources, test of emergency procedures, and a continuous training through drills and large-scale simulations. The higher the level of preparedness, the higher is the efficiency of response. The response phase aims at deploying on the ground the available resources properly managed by emergency management agencies, emergency services, and other actors that normally work in the disaster relief field, in order to rescue citizens and animals and keep infrastructures functioning. The scale of a disaster is bidimensional: it contemplates a temporal dimension, which explains how prolonged the hazard and the impact can be. It may vary from hours to days. For example, heavy rains can be lengthy, generating widespread floods. Once the response phase is completed, and all the survivors are safely sheltered, lifelines and infrastructures are brought back to normal functioning; emergency managers typically evaluate damages and needs of the population. The system is now moving forward to the recovery phase. *Recovery* is the fourth phase of the emergency management framework. Unlike for the response phase, recovery does not have a predetermined time slot: some countries, by law, define how long a response can be or what goals can determine the response concluded. Although mitigation, preparedness, and response might be efficient and might have reached predetermined goals, some level of damage still persists. That level of damaged should therefore be removed, and the normalcy will be re-established.

Recovery is complex and highlights the necessity of an integrated approach, a decision-making process, and the participation of diverse stakeholders (Haddow et al. 2002). Federal or national, state, and local governments usually plan for each one of the four phases of the framework, in order to have a well-established plan of action, which sets priorities and steps when the situation requires.

The Federal Emergency Management Agency (FEMA 2016), which is the agency mandated of planning and responding at the federal level, has recently updated the National Disaster Recovery Framework (NDRF, 2nd edition). The document organizes processes and capabilities for effectively managing resources and establishing the best path to a successful recovery (FEMA 2016). The framework applies the concept of "whole community approach" in order to "restore, redevelop, and revitalize the health, social, economic, natural, and environmental fabric of the community." FEMA stresses the "whole community

approach" as a holistic approach, where citizens, businesses, nonprofit organizations, and all level of governments partner together to achieve successful results and outcomes.

Disaster Recovery: Theory and Research

Disaster recovery is commonly defined as a return to normal conditions after the occurrence of a disastrous event that disrupted the environment, the human life, and the social and the economic fabric. Some scholars have defined different stages of recovery. Quarantelli (1999) has found that there are different ways of naming this process, which might be different in particular aspects. The five terms identified through a rigorous bibliographic research are the following: (1) reconstruction, which focuses more on rebuilding infrastructures; (2) restoration, which presumes that a physical or social element is put back at the pre-impact stage; (3) rehabilitation, similar to reconstruction but focuses more on people than the built environment – in this case mental health is considered; (4) restitution, which seems to be more giving back something to the rightful owner through legal ways; and (5) recovery, which aims to find some level of acceptability after a disaster. Although research shows that different denominations exist, it is widely recognized that recovery is a process; this means that recovery takes place at distinct stages and presents different results and outcomes; and key elements play critical roles in achieving successful recovery. For its complexity, the recovery process impacts on the environment and human systems, the political sphere, the organizational capabilities, and the bureaucratic machine.

Recovery has also been explained through different theoretical frameworks. Throughout the recovery process, a multitude of elements or systems interact; some theories have been applied to understand the mechanisms that underlie the recovery process. Phillips (2015) presented an overview of the most widely accepted theories and applied them to the concept of recovery. *System theory* argues that the built, the human, and the natural environment are interconnected and dependent. After a disaster each one of the systems might be affected, resulting in impacts also on the other systems. Under systems theory, recovery would be effective if the dependencies and the interconnections disrupted are restored. *Vulnerability theory* focuses on those who are more at risk, claiming that within the society some individuals are more at risk than others. The recovery process, under this lens, should place emphasis in recognizing that vulnerabilities exist and are constituted by economic, gender, and race issues. The opportunity during the recovery process is to recognize these vulnerabilities and address them during the process, creating safer conditions for citizens.

As Phillips (2015) points out, disasters also impact on social interactions. The *sociopolitical-ecology theory* (Phillips 2015) explains how interactions within the human sphere influence the capability for humans to recover. The recovery process might witness a competition among groups to obtain more resources; there might be an imbalance of power, leading certain groups to have easy access to resources or impede others to obtain what they need. Under this theory, the recovery process should rebalance the power, reduce discrimination and corruption, and allow those affected to take part in the process.

When a disaster occurs, all the elements that constitute the society are affected. Within the society the bureaucratic machine can be affected. The *emergent norm theory* (Phillips 2015) considers the insufficient level of preparedness of the administrative structures for new types of events and the increasing number of organizations that step up on the stage to address the unmet needs that the ordinary administrative system is not capable of satisfying. This is the case of the numerous long-term recovery groups and emergent groups (Stallings and Quarantelli 1985) that appear after a disaster and work to achieve a successful recovery.

In post-disaster recovery, affected communities are not only hardly hit from a "damaged infrastructure standpoint"; they are predominately affected from a "sociocultural-economic standpoint." A very novel approach to explain how certain communities recover better than others,

and sometimes stronger than others, has been explained by understanding what makes a community well tied. The application of the concept of *social capital* as one of the many factors that facilitate recovery has shown that communities with high level of social capital can recover to normal life, better than others. *Social capital* has been defined in several ways, but in sum, it entails a set of norms, values, social structures, and social networks (Bourdieu 1986; Coleman 1988; Puttnam 2001) that citizens rely on in order to bond together and work together to solve problems; social capital exists when community members establish mutual trust, collaboration, and participation (Nakagawa et al. 2004). Some studies have shown how communities, having high social capital, have recovered to normalcy (Aldrich 2011; Nakagawa et al. 2004).

Key Operations in Disaster Recovery: Debris Removal, Shelter/Housing, Damage and Needs Assessment, Infrastructures, Financial Assistance

Disasters wreak havoc. Depending on the extent and the severity of the event, damage sometimes can be very substantial. After a disaster, local, state, and federal agencies coordinate to provide immediate assistance to citizens. As situation stabilizes, public officials are deployed on the ground to initiate a damage assessment that includes assessment of infrastructures and their level of damage and functionality (roads, lifelines, transportation, communication systems). Infrastructures, such as roads and bridges, are essential for accessing communities and delivering livelihoods and other materials. Without electricity, water, and gas, communities cannot perform daily activities: water is necessary for drinking and for personal hygiene. Electricity keeps communication systems up and running but is also necessary to families for cooking and heating. Once damage assessment is completed, public officials plan primary actions to speed the recovery of the damaged critical infrastructures and lifelines, by setting up contracts, generally with local private companies and contractors.

After a disaster, urban areas are inundated by a huge amount of debris. As Phillips (2015) points out, debris can be disaster-specific and require careful removal. Some debris might lead to dangerous ashes (asbestos) that threaten human life. Debris removal should be planned ahead, in order to identify specific areas that can collect debris. Some countries have issued specific regulation for managing debris after disasters. For example, the Italian Civil Protection Department (DPC) has issued a specific ordinance considering debris as special waste and delegating to regions the duty of managing debris removal and stock and, when possible, the recycling of materials, also contracting out to selected private companies. In addition, debris removal should comply with health and safety policies (Phillips 2015).

Sheltering and housing are critical actions that public managers must plan, if not ahead, right after a disaster. Sheltering operations have a variable span of time: it can vary from a week to more than a month; this is a rough estimate, because there are a range of circumstances that can impact on the time: time for moving to temporary houses, bureaucratic processes, and the geography of places. Sheltering should give the first point of relief for citizens that lost their own houses, providing comfort, food, clothing, special supplies, and emotional support. Sheltering is sometimes coordinated by emergency management agencies and large nonprofit organizations that deploy volunteers to open shelters in public schools, libraries, and other locations previously identified during the planning phase. Housing solutions come next; these can be described as temporary and permanent. Temporary housing provides families with a safe place to return to normalcy. Temporary housing presents various forms of lodging: rental units and mobile homes. Rental units can be houses or apartments. Families can autonomously find temporary solutions and apply for rental assistance. Rental units must accommodate needs and be affordable (Phillips 2015). Mobile homes are the second recovery solution for families and homeowners. Mobile homes are simple structures that can be easily moved where necessary. Mobile homes are not suitable for every place, since planners should identify safe areas

where these units can be allocated (Phillips 2015). Both rental housing and mobile homes, although suitable recovery solutions, sometimes present challenges for individuals: people with physical disabilities will find it hard to walk on stairs; or living in a mobile unit might not be suitable for everybody. In this perspective, recovery managers should identify needs and appropriately assign housing solutions to applicants.

In the immediate aftermath of an event, communities are severely impacted, and daily routines are disrupted. Families might lose their house; workers might quit their job because their business had to be shut down. There are specific needs that public officials and voluntary organizations must assess and evaluate and subsequently work to satisfy. Needs assessment is a systematic process to identify gaps between what is necessary and what is the actual condition. This process should take part immediately; generally, agencies perform needs assessment as the situation stabilizes. Key factors that must be considered in carrying out the assessment comprise full information about family status, health conditions, income conditions, immigration status, and language barriers that might impede families to apply for the proper assistance. During the recovery phase, agencies and nonprofit organizations set up an unmet needs committee, with the purpose of finding ways to help community members get the necessary means when they do not meet federal guidelines or do not have sufficient resources to get to ordinary life (Phillips 2015).

An essential aspect of every recovery process is the availability of financial resources and the identification of various streams of funding. Disbursing monetary resources requires careful planning, making sure that applicants will receive proper assistance. There is specific sequence of delivery that FEMA sets up right after a disaster; this sequence delineates all the steps that survivors should follow to get help. In the first place, voluntary agencies provide emergency relief items and food. Homeowners then apply for receiving financial assistance from insurance companies and the National Flood Insurance Program (NFIP). Then, citizens must apply for FEMA assistance that will provide economic resources for temporary lodging expenses, repair or replace assistance, and permanent or semipermanent construction. Besides FEMA's assistance, there are other state or agency supports that can provide economic means to citizens. One of these is the Small Business Administration (SBA) loans, through which applicants can get up to $200.000 for repairing properties. When citizens cannot cover all the expenses although they received the maximum allowed, FEMA can refer applicants to voluntary agencies, and unmet needs committees can determine the necessities and the amount of money they can provide.

Planning for Recovery

Emergency managers and planners in time of "peace" undertake a set of coordinated activities that establish tactics, strategies, and desired outcomes. The federal government and each single state emergency management agency have a branch mandated of planning and setting guidelines for disaster recovery. Disaster recovery plans lay out a well-established set of operations focusing on the state's capabilities of carrying out timely restoration, the backing up to normal operations of all the critical infrastructures (usually coordinated with private sector), the provision of housing, and the economic as well as social fabric of the affected communities.

FEMA's National Disaster Recovery Framework (NDRF) is a platform for the whole community that sets out the core principles and practices for building, sustaining, and coordinating the delivery of recovery capabilities (FEMA 2016).

FEMA's NDRF identifies the Recovery's mission as the functional area that will define the capabilities necessary for an affected community to rebuild the critical infrastructures, to provide immediate and adequate long-term housing, to provide livelihoods to sustain survivors' needs, to support health and well-being of the community, and to promote sustainable economic development.

Also, the NDRF emphasizes coordination among actors and identifies the major players that will carry out the recovery operations. The

Recovery Framework highlights eight core capabilities, and five are specific to recovery: (1) economic recovery, (2) health and social services, (3) housing, (4) infrastructure systems, and (5) natural and cultural resources. In addition, the NDRF emphasizes that local governments set up a local recovery office and state agencies provide adequate resources and necessary support to local governments.

A critical component of every recovery plan is the identification and the inclusion of the whole community, with its primary actors: individuals, families, homeowners, nonprofit organizations, and private sector. At the local level, municipalities have the primary responsibility of managing recovery efforts, with the support of state and federal agencies. Every plan must highlight the coordination structure: for example, in a state plan, the managing agency will identify the actors (NGOs, private, federal agencies) and how they will deliver assistance to local recovery agencies. Generally, states support local government when local resources are not enough or are exhausted or when resources are not available. The same goes with states that can request additional resources to the federal government or to other states through the Emergency Management Assistance Compact (EMAC). The state emergency management agency is responsible for managing state support operations and resources and, when in need, requests more resources to the federal government.

A good recovery plan should comply with the federal guidelines and be consistent with the Presidential Policy Directive 8 (PPD-8), Homeland Security Presidential 329 Directive 5 (HSPD-5), and National Incident Management System (NIMS). State and local planning must ensure that each one of the five core capabilities has a robust set of procedures that will ensure a timely start of recovery operations following the response phase. For every recovery function, FEMA and state agencies identify key agencies that are responsible for coordinating the delivery of resources, the implementation of planned procedures, the assessment of communities' needs, the evaluation of the recovery process, and the communication with partners and communities.

Economic recovery "is the ability to return economic and business activities (including agricultural) to a state of health and develop new economic opportunities that result in a sustainable and economically viable community" (FEMA 2016). State and local agencies will plan in order to identify critical economic sectors that sustain the communities and will identify and prioritize the distribution of available resources to the various stakeholders.

Infrastructures systems: the recovery function will ensure that critical infrastructure systems will be timely and efficiently restored and services will be provided to communities. In this regard, agencies must delineate a timeline according to which public and private sectors will operate and will ensure that lifelines and transportation systems are restored.

Health and social services: healthcare and social services are critical for an affected community. Without the proper functioning of social services, the well-being of a community is at risk. Planning the recovery of social services requires that agencies identify and assess primary needs and prioritize and coordinate actions with state and local service providers in order to restore social and health services and meet the need of the population.

Housing: housing is critical for a community during the recovery process. State and local agencies must plan for finding solutions that will support the needs of the whole community. As FEMA (2016) states, housing is critical and challenging: agencies must ensure adequate, affordable, and equitable housing solution and deliver all the available resources in order to provide housing solution to renters and homeowners. Housing function will identify temporary/transitional housing solution and subsequently long-term housing restoration.

Natural and cultural resources: the recovery function is also responsible for assessing the damage of natural and cultural resources. Natural environments and historical landmarks might be heavily damaged by disasters. Consequently, agencies must plan procedures that will support the preservation and restoration, through technical assistance, of areas and facilities damaged.

Recovery managers must identify available monetary resources that will support recovery capabilities in order to develop protection and recovery strategies.

Stakeholders and Actors in Recovery: Public, Private, and Nonprofit – Donation Management

FEMA's "whole community approach" emphasizes that all the parties involved in planning and responding to disasters have to work together to achieve greater and better outcomes. At every stage of the emergency management framework, public agencies and stakeholders share experience and knowledge to address the necessities that can arise in the pre- and post-disaster time. The recovery timeframe requires increased efforts to collectively meet communities' needs.

Actors that work together for a greater good comprise public agencies, the private sector, and the nonprofit sector.

Emergency management offices and other public agencies are in charge of operating recovery plans and managing projects. Also, they are responsible for financing operations and disbursing financial resources for homeowners, to repair and rebuild, and for businesses to restart their daily operations. If businesses need money, they can apply for Small Business Administration's (SBA) loans, at very low interest rates.

Public agencies can contract with private companies to restore critical services (power lines, etc.) or, as the case of New Jersey after Sandy, have contractors run the entire recovery programs. Unfortunately, NJ state received much critique when hired private contractors are paying out a colossal amount of money. However, private companies are critical in providing or tapping into specific services that cannot be otherwise provided by state or local agencies, for example, insurance companies and banks. Insurance companies, after the assessment of damage, pay out homeowners when they file a claim and banks can provide loans. One important service that the private sector keeps providing after disasters is transportation. Private companies can support transportation operations (daily transportation; moving goods) by contracting with public agencies.

The nonprofit sector is probability the biggest slice of the cake in terms of personnel and resources. Only in the USA, more than 1.8 million nonprofit organizations run daily services for communities. (Guidestar (2018): retrieved from https://www.guidestar.org/Home.aspx.) Many of these organizations have a disaster response/recovery mission. Among these, the Red Cross, the faith-based organizations, and the community-based groups respond to emergencies by running sheltering operations, providing food and livelihoods, assessing needs, and restoring and rebuilding houses.

After a disaster, there is an outpouring generosity. People donate goods and money to organizations; private foundations raise money for the nonprofits to be used for recovery projects. Donations management is sometimes burdensome and requires trained staff. Nonprofit organizations are held accountable for the money they spend and provide to citizens. During those times, material donations can be of obstacle. People tend to donate all the sort of goods sometimes not necessary research showed (Holguín-Veras et al. 2014), that material donations can complicate response efforts, news media and organizations are increasingly asking for money instead of material goods.

Integrating Mitigation into Recovery

As a community recovers from a disaster, emergency managers and city planners should consider strategies that integrate mitigation practices in order to reduce impacts of future events. Public officials should prepare a specific action plan that delineates what the future community would look like and ways they want to reduce as much as possible any likely damage. The mitigation plan's role is twofold: first, it serves as a document that encompasses a thorough risk analysis, including socioeconomic data of communities; second, it should be a regulatory document that will regulate any future project when it comes to rebuild or develop new areas.

After a disaster, there is a general concern for communities to rebuild as quickly as possible, avoiding lengthy processes and harsh public discussions that will likely hamper the ability to restore the original conditions. But sometimes building quickly is not the best strategy to adopt. There serious considerations that must be made based upon these questions: Do I rebuild? Do I relocate? And if so, where?

It is normal that survivors want to rebuild in the same place, because there is always a certain level of place attachment that keeps them in the same place. Or citizens recognize that rebuilding in the same area is not convenient and prefer to relocate. Relocating also raises the question whether move to a newly developed area or relocate in the closest urban area. Rebuilding in the same place should be done, only if the new project is compliant with the regulations that the mitigation plan imposes and according to strengthened building codes that the municipality should have designed in the new development plan. Survivors that relocate to a newly developed area should consider whether the new house is located in a low-risk area and all protective measures are adopted. Relocating in the urban areas can create some challenges. Word a part for relocating in the urban area. This solution is practical only if there are enough houses to be sold or rent; it is desirable if the urban area had little to no damage. And it is desirable because it can be less costly and economic development can benefit.

Since housing solutions are the main concern of emergency managers and city planners, a mitigation plan for future development should integrate how new lifelines will be built and made stronger to sustain impacts. For example, with high-speed winds and heavy rains, power lines can be severely damaged. The restoration of new power is costly, but adopting in-ground solutions (this happens in the majority of European countries) can reduce the likelihood that aerial power lines break down.

Public Participation in Disaster Recovery

Communities that are impacted by disasters are always encouraged to participate and design a recovery process. Engaging the whole community is central to the new approach to emergency management and especially to the FEMA's "whole community approach."

Public participation processes have been central to the large hazard mitigation planning literature, response and organizational behavior, collaborative processes, and less explored during disaster recovery processes. For example, Burby (2003) showed how collaborative and participative processes led to better planning procedures. Public participation is important for several aspects. First, citizens know the context of their communities and neighborhoods: they have knowledge of the social dimensions in which they live and all the critical factors that influence their communities (family status, poverty, etc.). The knowledge citizens have is an extremely valuable information for public officials when planning for recovery actions.

Second, participating in recovery and decision-making processes gives the right to citizens to express opinions and comments on projects. Depending on the level of participation, public officials can integrate proposed ideas for the establishment of priorities and delivery of resources, the satisfaction of primary needs, and the design of projects for restoring and developing the whole community. It must be clarified that every public participation process is composed of different factors: (1) a level of power held by the public official, (2) a level of power given to the community, and (3) consultation and negotiation practices.

Even if the public participation represents a high democratic value, integrating and designing participatory processes do not come always easily. First of all, public officials should understand what best participatory practice they can adopt. Participatory processes range from no or limited participation (citizens listen) to high involvement (citizens comment; express opinions; decide). Second, public officials must understand that a community presents a broad range of stakeholders, each one with different interests. Balancing all the interests presents a challenge that managers must confront. Third, public officials must choose the best participatory practice:

these include focus groups, advisory committees, forums, workshops, etc. Whatever the chosen techniques is, public officials should be able to keep a two-way and open communication with citizens at all times.

Public officials should be aware that failing in integrating public participation processes is easy. Regardless the techniques, public officials are required to communicate constantly with citizens and share important and useful information; otherwise the recovery process will not receive adequate public attention and support. Sharing information with the community is vital, and for this reason public officials should adopt the best strategy even when conditions do not allow, e.g., power outage.

In the recovery planning phase, public official should keep strong relationships with stakeholders, community leaders, and organizations, in order to collect critical information regarding their community, such as unemployment and poverty levels, minorities and underrepresented social groups, and people with disabilities.

Conclusion

Disaster recovery is mostly known as a concerted set of action aimed to restore pre-disaster conditions. Although this definition might not be quite exhaustive, research is still trying to define a theory of disaster recovery.

The post-disaster timeframe is characterized by extreme challenges, for which disaster recovery mangers have responsibilities to at least minimize. However, disaster recovery is a critical phase that can contribute to a new normalcy, when pre-disaster conditions cannot be restored.

After a disaster, recovery managers run operations that span across a broad range of sectors that include housing rebuilding, to business recovery, to critical infrastructures restoring. As all this operations are common during the recovery phase, planners and emergency managers should take advantage of normal situations and start planning for recovery. Planning is critical, because enhances public agencies' capability to effectively and efficiently run recovery operations, as well as, foresee necessary changes and measure to reduce impacts of future hazards as well as increase resilience of local communities.

Cross-References

▶ Natural Hazards

References

Aldrich, D. P. (2011). Fixing recovery: Social capital in post-crisis resilience. *Studies in Emergent Order, 4*, 58–68.

Bourdieu, P. (1986). The forms of capital. In *Handbook of theory and research for the sociology of education* (pp. 241–255).

Burby, R. J. (2003). Making plans that matter: Citizen involvement and government action. *Journal of the American Planning Association, 69*(1), 33–49.

Coleman, J. S. (1988). Social capital in the creation of human capital. *American Journal of Sociology, 94*, 95–120.

FEMA. (2016). National disaster recovery framework. *Fema*, June, p. 116.

Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2002). *Introduction to emergency management*. CRC Press.

Holguín-Veras, J., Jaller, M., Van Wassenhove, L. N., Pérez, N., & Wachtendorf, T. (2014). Material convergence: Important and understudied disaster phenomenon. *Natural Hazards Review, 15*(1), 1–12.

Nakagawa, Y., Shaw, R., & Khan, M. A. (2004). Social capital: A missing link to disaster recovery. *International Journal of Mass Emergencies and Disasters, 22*(1), 5–34.

Phillips, B. D. (2015). *Disaster recovery*. CRC Press.

Puttnam, R. D. (2001). *Bowling alone. The collapse and revival of American community*. Simon and Schuster.

Quarantelli, R. L. (1999). The disaster recovery process: What we know and do not know from research. Preliminary paper No. 286. *International Forum on Civil Protection*. Retrieved from http://dspace.udel.edu:8080/dspace/bitstream/handle/19716/309/PP286.pdf?sequence=1

Stallings, R. A., & Quarantelli, E. (1985). Emergent citizen groups and emergency management. *Public Administration Review, 45*(Special Issue 1985), 93–100.

Further Reading

Schwab, J., Topping, K. C., Eadie, C. C., Deyle, R. E., & Smith, R. A. (1998). *Planning for post-disaster recovery and reconstruction* (pp. 483–484). Chicago, IL: American Planning Association.

Phillips, B. D. (2015). *Disaster recovery*. CRC press.

Smith, G. (2012). *Planning for post-disaster recovery: A review of the United States disaster assistance framework*. Island Press.

Emergency Management: Shelter In-Place

Michael K. Lindell
Department of Urban Design and Planning, Institute for Hazards Mitigation Planning and Research, University of Washington, Seattle, WA, USA

Keywords
Structural resistance · Air infiltration · Air exchange · Dose reduction · Shelter in-refuge

Definition

Shelter in-place consists of remaining in a location, usually a structure, that provides greater protection against an environmental hazard than being outdoors. Shelter in-place is appropriate for situations when the shelter location provides adequate protection against hazard exposure but also might be chosen when insufficient time for evacuation would lead to being exposed to the hazard in a vehicle that provides even less protection than the shelter location.

Introduction

The essential distinction between shelter in-place and evacuation is that the former generally provides protection by shielding from a hazard, whereas the latter provides protection by distance from the hazard. There is a variation on shelter in-place, shelter in-refuge, that can be used when there are nearby locations that are safer than the locations where people find themselves when they recognize the need to take protective action. For example, a coastal community at the tip of a peninsula might have a tsunami vertical evacuation shelter that can be reached much more rapidly than evacuating to high ground at the base of that peninsula.

There are three major mechanisms by which sheltering in-place provides structural resistance against environmental hazards such as tornadoes, hurricane wind, wildfires, inland floods, storm surges, tsunamis, earthquakes, volcanic eruptions, and hazardous materials releases. First, a shelter can provide protection against the extreme pressure of wind and water hazards or against the extreme temperature of wildfires. Second, a shelter can provide protection from inhalation of hazardous materials such as toxic chemicals or volcanic ash. Third, a shelter can provide protection from direct radiation produced by an overhead plume or ground deposition of radiological materials.

Protection from Extreme Pressure or Temperature

Regarding the first mechanism, protection from wind and water pressure or from fire temperature, structures can lack resistance to environmental hazards because of inadequate designs, inadequate construction materials, or both (AIA 1995; IBHS 2007). In high wind (including tornadoes and hurricanes) and explosions (usually technological in origin, but also including some volcanic eruptions), a substantial increase in air pressure can cause structures to collapse. *Fortified* homes (https://disastersafety.org/fortified/) have connections and braces that reinforce roofs and gable-end walls against wind attack. In addition to positive pressure on upwind walls, high wind creates negative pressure, or suction, as it is forced to flow up and over the roof. This suction is greatest in flat roofs, intermediate in gable-end roofs (which slope in two directions), and least in hipped roofs (which slope in four directions). Suction tends to lift the roof from the walls unless resisted by adequate connections to the walls – which in turn, must have adequate connections to the foundation. Adequate designs and materials also provide protection to building openings such as windows and doors, thus preventing the wind from pressurizing the interior and adding to the stress on roof and walls. There is a need for window and sliding glass door shutters to resist the direct pressure of the wind and the impact of flying debris. However, door reinforcement is also important – especially for double-wide (two car) garage doors that are highly susceptible to failure

because their great width allows the wind to deflect them inward and pull the rollers out of their tracks.

Both riverine flooding and hurricane storm surge require the structure to have foundations anchored deep enough to resist scouring by water currents that can undermine building foundations and cause structural collapse. In addition, structures on the open coast must be of sufficiently sturdy construction that they can resist the direct impact of storm surf and battering debris from structures that have already been destroyed. Additional protection can be provided by floodproofing that uses waterproof construction materials, sealing of cracks, provision of valves on sewer lines, steel bulkheads for lower-level openings, and sump pumps to eject seepage. Tsunami impact poses an even greater threat than inland flooding or storm surge. These sea waves can threaten areas as much as 100 feet (30 m) above sea level, so destruction is highly likely for most structures located very near the shoreline. However, properly designed steel-reinforced concrete structures located a short distance inland are likely to resist even the largest tsunamis.

Wildfire hazard requires fire-resistant structures whose exterior walls are constructed of nonflammable materials such as metal, concrete, or masonry, and whose and roofs are metal or tile (see NFPA 2018). In addition, wooden doors should be replaced with metal ones, tempered glass should be installed to protect windows, and vents should be covered by metal screens. Such structures should be surrounded by a *defensible space* that is created by clearing vegetation from a 30 foot (9 m) perimeter around any structure, choosing fire-resistant plant varieties, and maintaining landscapes to reduce the buildup of flammable materials such as dead leaves and fallen branches (IBHS 2007).

Protection from Inhalation Exposure

The principal sources of inhalation hazards are airborne toxic and radiological materials (USEPA 1987). An enclosed space will resist infiltration if it can be closed tightly enough to keep out the hazardous material and has enough oxygen to sustain those within it until the danger has passed. Unfortunately, most structures are leaky, allowing contaminated air to infiltrate even when the doors and windows are closed. The rate of air exchange increases with the amount of leakage area, the wind speed, and the temperature differential between the indoor and outdoor air (Sorensen et al. 2004).

The rate at which indoor and outdoor air are exchanged is commonly measured in air changes per hour (ACH). However, emergency managers will find it more useful to think of air exchange in terms of turnover time, which is the reciprocal of the air exchange rate, or $t_B = 1/ACH$, where ACH is the number of air changes per hour (Mannan and Kilpatrick 2000). As Wilson (1987) emphasizes, an infiltration rate of 1.0 ACH does not imply that all the clean air will be gone in 1 h. Rather, the proportion of contaminated air gradually rises until 63% of the original air has been replaced by contaminated air at the end of 1.0 t_B hours and 95% of the original air has been replaced by the end of 3.0 t_B hours. Thus, for the case of 1.0 ACH, it will take over 3 h (not just 1 h) for the indoor air to become almost completely contaminated. This result is extremely important because it indicates that in-place sheltering is more effective than most people might infer from the apparent implication of the number of air changes per hour. The reason for the difference between the apparent result and the correct result can best be illustrated by examining the difference between the apparent, but incorrect, mechanism of air exchange and the actual mechanism. It would only take 1 h to replace the clean air (the incorrect result) if the contaminated air somehow "pushed out" the clean air, but this is not what happens. Rather, the contaminated air that infiltrates the structure mixes with the clean air rather than "pushing it out." Clearly, exfiltration of a mixture of clean air and contaminated air will take longer to exhaust the clean air in a structure than will exfiltration of ("pushing out") clean air alone. Consequently, sheltering in-place is at least three times as effective in reducing inhalation exposure as it might appear to be.

Although this time lag effect is important, it is not the only mechanism by which sheltering

in-place can reduce adverse health effects; there is also a damping effect that reduces the peaks in plume concentrations. The fluctuations in wind speed and direction that produce these peaks arise from irregularities in meteorological conditions and local terrain. One way of measuring peak concentration is by estimating the value that is exceeded approximately 1% of the time. Wilson (1987) reports that in the outdoor (contaminated) air, such 1% peak concentrations are 400% as large as the mean concentration. For indoor air, the equivalent peak concentration is only 50% larger than the mean. This is, of course, of considerable significance when peak concentrations are the principal health threats.

As Wilson (1987, 1989) and others have observed, a major problem in assessing the effectiveness of shelter in-place is uncertainty about whether indoor air concentrations will remain sufficiently low for a sufficiently long period of time. This can be answered definitively only if there is information about the hazardous material being released (especially the identity of the material released, and the rate and duration of the release), local weather conditions (wind speed, wind direction, and atmospheric stability), and the air exchange rates for the structures in the hazard impact area. Data on the release and the meteorological conditions are not available until an incident occurs, but data on air exchange rates can be collected in advance. First, Rogers et al. (1990) report that energy conservation research has shown air exchange rates in most US dwellings range from 0.5 to 1.5 ACH. Second, Wilson (1989) reports that the most important factor affecting a structure's air exchange rate is its leakage area, which is substantially determined by the presence of a vapor barrier in the walls and ceiling of a structure. This is a feature that is most common in houses built in cold climates after 1960. Thus, emergency managers can estimate the effectiveness of sheltering in-place in their communities by obtaining local utilities' data on the age of the housing stock within different neighborhoods, focusing especially on neighborhoods with older, smaller homes occupied by low-income households (Chan et al. 2007a, b). Special facilities, especially those such as hospitals that have low mobility residents, should be examined individually to assess their air exchange rates.

Protection from External Radiation Exposure

In addition to being an inhalation hazard, a plume of radioactive material can cause harm by means of external gamma radiation from the cloud and from ground contamination. Dense building materials such as concrete, brick, and stone provide shielding from external gamma radiation and, thus, can provide a basis for sheltering in-place during radiological emergencies. The effectiveness of structures made from different types of building materials has been examined in number of research studies (see Lindell et al. 2006, for a summary). These studies calculated the dose reduction factors (the ratio of the dose received while sheltering to the unprotected dose) for three exposure routes: external gamma radiation from the cloud, external gamma radiation from ground contamination, and inhalation of radioactive materials infiltrating into the structure. Burson and Profio (1977) found that sheltering in a wood frame dwelling provides little more protection from cloud and ground exposure than does "sheltering" in a vehicle while evacuating. Sheltering on the ground floor of a masonry home with no basement or in the basement of a wood frame home gave considerably higher levels of protection: about 50% of the unprotected exposure to the cloud and less than 20% of the unprotected exposure to the ground. As one might expect, the basement of a masonry house was even more effective: 40% of the cloud exposure and 5% of the ground exposure. A large office building was the most effective shelter of all, reducing cloud exposure to about 20% and ground exposure to 1%.

McKenna (2000) reported the results of an extensive series of analyses by the Nuclear Regulatory Commission, which examined the relative effectiveness of continuing normal activity, sheltering in a home basement or large building, or evacuating before or after plume arrival at three distances from the plant. These analyses confirmed the results of earlier studies by finding that even a late evacuation is better than home shelter, large

building shelter is better than late evacuation, and early evacuation is best of all. Thus, those who are within 5 miles of a nuclear power plant have high vulnerability if they remain in their homes during a release. Only large building shelter provides as much safety as early evacuation.

Implementing Shelter In-Place

The steps required to implement shelter in-place vary somewhat by hazard. There is usually no forewarning for earthquakes, so people can typically protect themselves only by sheltering beneath a sturdy piece of furniture ("duck, cover, and hold on") in the room where they are located when the shaking begins. There is usually more forewarning for tornadoes, so they can shelter in the basement or, if none is available, in an interior room. With forewarning of a hurricane, people can install shutters on windows and brace doors before hurricane wind becomes too strong. For a flood, they can fill and place sandbags before proceeding to an upper floor. For a wildfire, people can clear a defensible space before retreating inside. Finally, for toxic chemical releases, shelter in-place involves going indoors; closing doors and windows; turning off heating, ventilation, and air conditioning systems; and, if possible, taping the cracks around doors and windows – which takes approximately 17 min for a single room (Rogers et al. 1990). However, in chemical emergencies, it is also important for people to tune to the emergency alert system so they can receive further instructions about when to open doors and windows after the plume has passed (Sorensen et al. 2004). Airing out the structure immediately after plume passage is important because, at that point, the inside air is more contaminated than the outside air.

It is important to recognize that, in some hazards, people's decisions to shelter in-place are affected by their desire to protect property from hazard impact (Cova et al. 2009). For wildfire protective action decisions, the number of people who take this "stay and defend" option is a significant percentage of those at risk (McCaffrey et al. 2018). For other hazards, such as toxic chemical releases, property protection is not possible, so the decision to shelter in-place depends almost exclusively on people's perceptions of its efficacy in protecting people. In this case, a shelter in-place recommendation is likely to elicit low compliance (Sorensen et al. 2004), but compliance might be improved if authorities explain why shelter in-place provides effective protection and why evacuation might result in "sheltering" in a car when overtaken by a chemical plume.

Conclusions

Shelter in-place can be an effective method of protecting people from a variety of different environmental hazards. However, its suitability depends on the characteristics of the hazard, local weather conditions, and local building stock (including the variability in the shelter suitability among structures within the community). In addition, risk area residents' motivation to shelter in-place depends on their perceptions of its effectiveness in protecting persons and the degree to which it allows them to protect their property as well. Emergency managers need to thoroughly examine the feasibility of this protective action before an emergency occurs to ensure that a recommendation to shelter in-place will achieve a high level of compliance and will effectively protect the population at risk. It is especially important to develop procedures that identify in advance "who should be warned to do what and when" (Cova et al. 2017).

Cross-References

- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Evacuations
- ▶ Emergency Management: Preparedness and Planning

Acknowledgments This research was supported by the National Science Foundation under Grants CMMI-1760766 and CMMI-1826455. None of the conclusions expressed here necessarily reflects views other than those of the author.

References

AIA – American Institute of Architects. (1995). *Buildings at risk: Wind design basics for practicing architects*. Washington, DC: American Institute of Architects.

Burson, Z. G., & Profio, A. E. (1977). Structure shielding in reactor accidents. *Health Physics Journal, 33*(4), 287–299.

Chan, W. R., Nazaroff, W. W., Price, P. N., & Gadgil, A. J. (2007a). Effectiveness of urban shelter-in-place – I: Idealized conditions. *Atmospheric Environment, 41*(23), 4962–4976.

Chan, W. R., Nazaroff, W. W., Price, P. N., & Gadgil, A. J. (2007b). Effectiveness of urban shelter-in-place – II: Residential districts. *Atmospheric Environment, 41*(33), 7082–7095.

Cova, T. J., Drews, F. A., Siebeneck, L. K., & Musters, A. (2009). Protective actions in wildfires: Evacuate or shelter-in-place? *Natural Hazards Review, 10*(4), 151–162.

Cova, T. J., Dennison, P. E., Li, D., Drews, F. A., Siebeneck, L. K., & Lindell, M. K. (2017). Warning triggers in environmental hazards: Who should be warned to do what and when? *Risk Analysis, 37*(4), 601–611.

IBHS – Institute for Business and Home Safety. (2007). *Builder's guide.* Tampa: Author. Accessed 1 Nov 2018. http://disastersafety.org/fortified/safer-living/

Lindell, M. K., Prater, C. S., & Perry, R. W. (2006). *Fundamentals of emergency management.* Emmitsburg: Federal Emergency Management Agency Emergency Management Institute. www.training.fema.gov/hiedu/aemrc/booksdownload/fem/ or http://hrrc.arch.tamu.edu/publications/books%20and%20monographs/

Mannan, M. S., & Kilpatrick, D. L. (2000). The pros and cons of shelter-in-place. *Process Safety Progress, 19*(4), 210–218.

McCaffrey, S., Wilson, R., & Konar, A. (2018). Should I stay or should I go now? Or should I wait and see? Influences on wildfire evacuation decisions. *Risk Analysis, 38*(7), 1390–1404.

McKenna, T. (2000). Protective action recommendations based upon plant conditions. *Journal of Hazardous Materials, 75*, 145–164.

NFPA – National Fire Protection Association. (2018). *NFPA 1144: Standard for reducing structure ignition hazards from wildland fire*. Quincy: Author. Accessed 11 June 2018. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1144

Rogers, G. O., Watson, A. P., Sorensen, J. H., Sharp, R. D., & Carnes, S. A. (1990). *Evaluating protective actions for chemical agent emergencies* (ORNL-6615). Oak Ridge: Oak Ridge National Laboratory.

Sorensen, J. H., Shumpert, B. L., & Vogt, B. M. (2004). Planning for protective action decision making: Evacuate or shelter-in-place. *Journal of Hazardous Materials, 109*, 1), 1–1),11.

USEPA – US Environmental Protection Agency. (1987). *Technical guidance for hazards analysis: Emergency planning for extremely hazardous substances*. Washington, DC: US Environmental Protection Agency.

Wilson, D. J. (1987). Stay indoors or evacuate to avoid exposure to toxic gas. *Emergency Preparedness Digest (Canada), 14*, 19–24.

Wilson, D. J. (1989). Variation of indoor shelter effectiveness caused by air leakage variability of houses in Canada and the USA. In T. Glickman & A. Ujihara (Eds.), *Proceedings of the conference on in-place protection during chemical emergencies*. Washington, DC: Resources for the Future.

Further Reading

Cova, T. J., Dennison, P. E., Li, D., Drews, F. A., Siebeneck, L. K., & Lindell, M. K. (2017). Warning triggers in environmental hazards: Who should be warned to do what and when? *Risk Analysis, 37*(4), 601–611.

IBHS – Institute for Business and Home Safety. (2007). *Builder's guide.* Tampa: Author. Accessed 1 Nov 2018. http://disastersafety.org/fortified/safer-living/

Emergency Management: Spontaneous Volunteers in Response to Disaster

Lisa C. Orloff
Worldcares, New York, NY, USA

Keywords

Spontaneous volunteers · Disaster response · Disaster volunteerism · Community response · Convergence · Volunteer reception centers

Definition

Spontaneous unaffiliated community volunteers (SUCV) or just-in-time volunteers are defined as "citizens with knowledge of the area and ties to the community; they may or may not have training or experience in emergency response, but most possess skills from their everyday life experiences, job experiences, or experiences due to their responsibilities in running a household, managing volunteer responsibilities etc." (Orloff 2011, p. 83).

Introduction

Spontaneous volunteerism is a part of the history of disaster response (Katz 1989; Points of Light Foundation 2002). As long as there have been disasters, individuals and communities have emerged to help their neighbors and fellow human beings. For example, during the 1859 Battle of Solferino, Henri Dunant's spontaneous volunteer efforts led to the founding of the International Committee of the Red Cross. The human need to connect to others and help others in need is innate and has been demonstrated in a variety of disasters, such as the 1917 Halifax ammunition ship explosion, the September 11th attacks, Hurricane Katrina, and the 2011 Tōhoku earthquake and tsunami (Points of Light Foundation 2002).

Despite the natural inclination of human beings to respond to crisis, between 1978, when FEMA was established through the 2005 Hurricane Katrina response, spontaneous community volunteerism was considered a challenge and a hindrance by official disaster managers (Orloff 2011; Points of Light Foundation 2002, 2005). People coming out of their homes and places of work to help was often referred to as "a disaster with in a disaster" because these individuals and groups sometimes created management challenges for official responders. "When disaster strikes, emergency management and voluntary agencies automatically mobilize. Each has a specific role to help ensure a community's successful response to and recovery from the disaster's devastation" (Points of Light 2002, p.). These groups are trying to focus on helping the community with their own experienced workers but are now burdened with the task of simultaneously overseeing these spontaneous, unaffiliated volunteers (Points of Light Foundation 2002, 2005). This may mean using some of their staff to work with the volunteers rather than directly helping the victims.

In 2011, the perspective regarding who should and should not be involved in disaster response shifted. With an increase in frequency and impact of disasters, FEMA administrator, Craig Fugate, acknowledged the limits of the government in meeting the challenges posed by a catastrophic incident and accepted societal volunteerism (FEMA 2011). Subsequently, guides and playbooks and new approaches have been published to help individuals, communities, organizations, and government work together to achieve a whole of community approach to disaster response. This chapter will provide information regarding the various management methods in place to help agencies deal with spontaneous volunteers during disaster and provide concrete guidelines from the volunteer reception center (VRC) method that was implemented in 2011.

Management Methods

The most effective way to integrate spontaneous volunteers into the disaster response is by leveraging preexisting and proven management systems, including the National Incident Management System (NIMS), the Incident Command System (ICS), and the methodologies within them (Points of Light Foundation 2002). FEMA (2017) released a revised NIMS doctrine that provided "a common, nationwide approach to enable the whole community to work together to manage all threats and hazards" (para 1). NIMS applies to all incidents, from traffic accidents to major disasters, regardless of cause, size, location, or complexity (Haddow et al. 2017).

According to FEMA (2017):

> NIMS guides all levels of government, nongovernmental organizations (NGO), and the private sector to work together to prevent, protect against, mitigate, respond to, and recover from incidents. NIMS provides stakeholders across the whole community with the shared vocabulary, systems, and processes to successfully deliver the capabilities described in the National Preparedness System. NIMS defines operational systems, including the Incident Command System (ICS), Emergency Operations Center (EOC) structures, and Multiagency Coordination Groups (MAC Groups) that guide how personnel work together during incidents, from traffic accidents to major disasters. (para 5)

The ICS is a fundamental element of incident management under which command for disaster management, particularly, emergency preparedness and management, is centralized and

controlled through the EOC. The EOC allows the community businesses to continue functioning during the disaster. Coordination and support for disaster management comes from the MAC groups which combine people, processes, communication, equipment, and facilities into a common system.

The organization and terminology used by ICS facilitate its effectiveness (FEMA 2017). The structure of ICS corresponds with command, operations, planning, logistics, intelligence and investigations, finance, and administration functional areas as a means of enabling various groups to perform their tasks (FEMA 2017). By standardizing the management process, ICS allows the incident managers to determine which elements of the incident must be performed quickly. There are a variety of tasks that must be performed, including designating oversight of the incident; dictating which group reports to which agency; determining the optimal span of control (i.e., number of subordinates managed by a supervisor); and meeting twice daily with teams for briefings and debriefings. All of these crucial tasks culminate into a management system that can be applied to spontaneous volunteer and successfully applied to the management of the volunteer reception center as explained in the next section.

The Volunteer Reception Center (VRC) Model

According to Orloff (2011), the volunteer reception center (VCR) model provided both structure and planning for how to oversee spontaneous volunteerism during disasters. Table 1 presents the five different types of volunteers that are typically available during disasters. Each type offers a different set of skills and ties to the community and thus requires varying levels of supervision. There are fundamental elements of spontaneous volunteer management that are quite simple in philosophy but a bit more complicated to coordinate in reality. If an agency is seeking to manage spontaneous volunteers within an unfamiliar community, it is important to engage a trusted, local leader to act as a liaison. This individual will have the trust of the community and provide validation for the group wishing to organize the community.

Emergency Management: Spontaneous Volunteers in Response to Disaster, Table 1 Types of volunteers and their skills and community ties (Orloff 2011)

Type of volunteer	Description of skills and community ties
Agency-affiliated pre-trained volunteers	Volunteers are registered with your agency prior to disasters and have been through your agency's standards of background check, training, and credentialing as well as gained a history of volunteer service with your agency
Registered volunteers	Volunteers are registered through application, but may not have taken any of your agency's training or gained a history of volunteer service with you
Partnering agency-affiliated pre-trained volunteers	These volunteers have been trained by groups that you know in your community, such as faith-based organizations, the boy scouts, Lions Clubs, CERT teams, and PTA members. Affiliated volunteers with disaster management training may include those who volunteer for groups like The Salvation Army, United Way, Habitat for Humanity, and Doctors Without Borders
Spontaneous unaffiliated community groups	Many nonprofit groups do not have a disaster-related mission, but will find themselves and their constituency emerging to help in some way in the event of a disaster. Such groups may include faith-based groups, the national reserves, professional and trade-person associations, and clubs, such as rotary, Lions Clubs, and boy scouts, as well as businesses within your community, like Walmart or World Central Kitchen
Spontaneous unaffiliated community volunteers	Citizen in your community who have ties and knowledge of the area. They may or may not have training or experience in emergency response. Most volunteers do, however, possess skills from their everyday life experience, job experience, or experience due to their responsibilities in running a household, managing volunteer responsibilities, etc.

The VRC model "outlines the steps for the set-up of a room or building that will put a roof, both literally and functionally, over the Spontaneous Volunteer management process. . .including spot screening, selection, and placement of spontaneous volunteers This model can help to address the internal capacity challenges that emergency managers face, especially by drawing volunteers as additional capacity and resources to one central location to implement much of your volunteer management protocols and process" (Orloff 2011, p. 125). While there are several floor plans for a VRC, it is the management structure that is most important (Orloff 2011; Points of Light Foundation 2005). Once volunteers are engaged, either by spontaneously showing up or because an agency has solicited them, they must first be registered using either a registration form or a volunteer application. Next, volunteers should be interviewed in order to understand what skills they possess and how best these skills should be used. They will be matched to a specific role, such as ditch digger or which may require a short training session. If the VRC is deploying teams such as in a muck and gut operation post flooding, the volunteer is then paired with a team that follows the incident command structure that will include a team leader, a safety officer, and up to seven workers. The volunteer is then given personal protective equipment and other tools for the assigned role and a volunteer work order. The volunteer is then part of a team and would deploy into the field to conduct daily activity and return to the VRC to debrief and decontaminate.

Alternatively, a VRC will act as a coordination and referral center to match volunteers to agencies in need of volunteers rather than deploying teams directly into the field. In this case, the agency may have a desk in the VRC, or a person may screen and refer the volunteer to go to the agency where the agency processes are undertaken (Orloff 2011; Points of Light Foundation 2005). Voluntary agencies active in disasters can set up the VCR and also coordinate with their network partners through daily calls and reports into an operation center, where an individual representing voluntary agencies active in disaster has a seat. Timing is important as well given that when disasters occur, systems will not be in place or available, leaving a lag time. If there is urgency in needs or few resources available due to the disaster, various elements in the VRC, such as background checks of volunteers, may be skipped (Orloff 2011).

Building Resilience

The impact of disasters often leaves survivors with a sense of disempowerment. "After a disaster, the number of people with psychological trauma exceeds the number of people with physical injury by as much as 40 to 1' (Links 2017, p. 1). In particular, many people in the community have suffered loss of life and/or property and as a result them feel little control over the situation or their lives. Hence, spontaneous volunteerism is an instinctual way for people to regain control after a disaster and to build resilience during recovery (Steffen and Fothergill 2009). Active involvement in their own community allows these survivors to reposition themselves as volunteers and reconnect with other residents in a positive, prosocial and therapeutic manner that lasted post-disaster. According to Steffen and Fothergill (2009): "taking action facilitated meaningful therapeutic recovery from feelings of victimization following the event. In addition to the apparent long-term impact on personal healing, the opportunity to volunteer had lasting impacts on self-concept that translated to significant changes in life choices" (p. 29). Thus, volunteerism strengthened community relationships, which would be essential in neighborhoods where disasters commonly occurred (Links 2017).

Conclusion

According to The Borgen Project (2015), the average number of natural disasters, especially related to climate, has increased from 1970 to 2009, impacting millions of people worldwide. It is not sufficient to rely only on government resources when dealing with disasters, as shown by many of the catastrophes that occurred nationwide over the past 40 years (FEMA 2011) recognized that a government-centric approach to disaster

management was insufficient to meet the challenges posed by most catastrophic incidents occurring in the United States. Consequently, FEMA (2017) revised existing systems, including NIMS, ICS, and the VRC, in order for them to be available for adaptation in any circumstance. The VCR model, in particular, helped various agencies to supervise spontaneous volunteers in communities where disaster occurred and ensure that systems for preparation were in place beforehand, during, and post disaster that protected them from harm and supported community recovery.

Cross-References

- Emergency Management: Best Practices
- Emergency Management: Crisis Management and Response
- Emergency Management: International
- Emergency Management: Preparedness and Planning
- Emergency Management: Recovery
- Federal Emergency Management Agency
- Natural Hazards

References

FEMA. (2011). *A whole community approach to emergency management: Principles, themes, and pathways for action*. Accessed at: https://www.fema.gov/media-library-data/20130726-1813-25045-3330/whole_community_dec2011__2_.pdf (2/4/2019).

FEMA. (2017). *National incident management system,* 3rd ed. Accessed at: https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf (2/4/2019).

Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2017). *Introduction to emergency management* (6th ed.). Oxford: Butterworth-Heinemann.

Katz, J. (1989). *Shattered city: The Halifax explosion and the road to recovery*. Halifax, NS: Nimbus.

Links, J. (2017). *Predicting community resilience and recovery after a disaster*. Access at: https://blogs.cdc.gov/publichealthmatters/2017/08/predicting-community-resilience-and-recovery-after-a-disaster/ (2/4/2019).

Orloff, L. (2011). *Managing spontaneous community volunteers in disasters: A field manual*. Boca Raton, FL: CRC Press.

Points of Light Foundation. (2002). Preventing a disaster within the disaster: The effective use and management of unaffiliated volunteers. Access at: http: http://www.cert-la.com/downloads/education/english/disasterbook.pdf (5/10/19).

Points of Light Foundation. (2005). *Managing spontaneous volunteers in times of disaster: The synergy of structure and good intentions*. Accessed at: https://www.fema.gov/pdf/donations/ManagingSpontaneousVolunteers.pdf (2/4/2019).

Steffen, S. L., & Fothergill, A. (2009). 9/11 volunteerism: A pathway to personal healing and community engagement. *The Social Science Journal, 46*(1), 29–46.

The Borgen Project. (2015, June 14). *Are natural disasters increasing?* Accessed at: https://borgenproject.org/natural-disasters-increasing/ (2/4/2019).

Further Reading

Adams, R. E., & Boscarino, J. A. (2015). Volunteerism and Well-being in the context of the world trade center terrorist attacks. *International Journal of Emergency Mental Health, 17*(1), 274–282.

Chatham County Emergency Operations Plan. (2015). *Appendix 7–1: Disaster volunteer assistance and management plan*. Access at: https://www.chathamemergency.org/2015EMdocs/ESF%207%20ANX%20APP%207-1%20VRC.pdf (5/10/2019).

Solnit, R. (2009). *A paradise built in hell: The extraordinary communities that arise in disaster*. New York: Penguin Books.

Emergency Management: Working with Vulnerable Populations

Jennifer Mincin
Health and Human Services Department, SUNY Empire State College, Selden, NY, USA

Keywords

Aging · Disability · Immigrants · Refugees · Socioeconomic · Vulnerable populations

Definition

Emergency management situations often require that workers render aid to populations who have disabilities or are vulnerable. For purposes of this chapter, a person with a disability can be defined as someone who may function on a daily basis with little assistance to someone who may have

difficulty in performing functional tasks or daily living activities and generally meets the federal definition. The federal definition includes people with physical/functional disabilities as well as cognitive and emotional such as a learning or developmental disability and mental illness. People are considered to have a severe disability if they are unable to perform one or more of these tasks or activities, need personal assistance, or have one of the severe conditions described in the report. Vulnerable populations refer to people who have increased risk of disruption or death during and after a disaster including people living in poverty, immigrants and refugees, women and girls, and people with disabilities and the aging.

Introduction

This chapter discusses the disability and vulnerable populations in terms of how emergency managers, field personnel, and first responders interact with and support them during disasters and crises. Notably, this group requires greater assistance during emergency situations mainly because they lack access to a variety of things that most people take for granted, such as healthcare, employment, and school, and they have higher rates of poverty and suffer worse socioeconomic outcomes than those without disabilities (World Report on Disability 2011, p. xxi). These intersecting factors present an opportunity for emergency managers, field personnel, and disaster human service agencies to work with, support, and include and integrate people with disabilities and vulnerable populations into all phases of emergency management (mitigation, planning, response, and recovery). However, it is paramount that the emergency management field understands basic parameters and context in which people with disabilities and vulnerable populations live on a daily basis in order to better assist them when it is most critical. In particular, there are many individuals living independently with a disability or coexisting disabilities. In addition, there is a difference between people who have a disability and those who have a medical condition; it is important to keep in mind that because a person may have a medical condition, it does not mean she or he has a disability, though it could.

Understanding differences between "legally protected class" and identifying people with specific needs impacts the type of post-disaster services they may or may not be guaranteed. As per the Americans with Disabilities Act (ADA), persons with disabilities are a legally protected class (Older people are also a protected class under the Older Americans Act.) and can use the ADA as statutory authority for enforcement and lawsuits. An individual is someone with a disability if the following is true: he or she (1) has a physical or mental impairment that substantially limits a major life activity; (2) has a record of such an impairment, and/or; and (3) is regarded as having such an impairment (A Guide to Disability Rights Law 2009). According to ADA, the type of disabilities (including the age spectrum from pediatric to geriatric) are: (1) physical (e.g., severe arthritis, spinal cord injuries, people who use wheelchairs, people with multiple sclerosis); (2) sensory (e.g., people who are blind, deaf, hard of hearing); and (3) cognitive (e.g., people with mental illness, learning disabilities, mental retardation/developmental disabilities) (A Guide to Disability Rights Law 2009). In addition, to a person identifying as having a disability, it is equally important to recognize that some people are living with two or more disabilities. For example, there may be a person who is deaf and has a learning disability, who has cerebral palsy and general anxiety disorder, etc. The purpose of this chapter is to provide first responders with information on how to develop emergency management plans that will benefit disability and vulnerable populations in a crisis.

Disability and Vulnerable Populations

The ADA of 1990 does not specifically address the issue of compliance in emergency planning and response. However, it does mandate that all public and private sector facilities come into and remain in compliance, provide reasonable accommodations, and be accessible (Davis and Sutherland 2005). Per federal law, shelters and

other disaster-related services must be accessible to people with disabilities (FEMA 2010). In recent years, FEMA has provided clear written guidance on this including in shelters (FEMA 2010). Access must be both physical (e.g., architectural barriers) and programmatic. FEMA clarifies those with functional needs as:

> Functional Needs Support Services (FNSS) are defined as services that enable individuals to maintain their independence in a general population shelter. FNSS includes:
>
> - reasonable modification to policies, practices, and procedures
> - durable medical equipment (DME)
> - consumable medical supplies (CMS)
> - personal assistance services (PAS)
> - other goods and services as needed. (FEMA, Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters 2010, p. 8)

Populations who have special needs, including disabilities, comprise vulnerable populations, but are not protected legally in the way that ADA protect people with disabilities (Kailes and Enders 2006). According to the EAD Toolkit (2007), these groups include (list adapted from EAD Toolkit 2007): (1) Refugees and immigrants including documented and undocumented people; (2) non-English speaking/English proficiency including those whom English is not their first language as well as individuals who have low English comprehension/literacy issues either because of or not because of a cognitive disability; (3) homelessness and disability issues, specifically mental illness and physical disabilities; (4) low income; and (5) residential care facilities that may include nursing homes, assisted living centers, drug treatment centers, group homes, residential homes, foster homes, adult and childcare facilities, etc. Health and Human Services (HHS 2006) specified that anyone who may be at risk because of their age, status, or physical condition would be considered to have special needs during public health emergencies.

The broad nature of the usage of the term "special needs" or vulnerable populations can lead to confusion during and after a disaster. During the 2007 California wildfires, confusion regarding the term special needs hindered the response. According to the After Action Report authored by Kailes (2008), "The term 'special needs' does not work because it does not provide guidance to operationalize needed planning tasks. A better way to think about the needs of people with disabilities and activity limitations is to use a function based orientation that considers major functional needs: communication, medical, maintaining functional independence, supervision, and transportation" (p. 33).

Age

First responders should note that a person's age, whether juveniles (not yet 18) or adults beyond middle age, is linked to vulnerable populations and disabilities. Prior to adulthood, children and adolescents do not have the cognitive capacity to deal with emergency situations and very young children (infants through preschool age) have limited physical capacity as well.

Similarly, older people are likely to have physical and/or cognitive disability. The US Census (2017) indicated that there were 47 million Americans aged 65 and older, with approximately 75% claiming to have one or more disabilities. The number of people over 60 with disabilities is expected to grow as the Baby Boomer generation (born 1940 through mid-1960s) ages. The location in the United States of residents may also be relevant, particularly as there are large aging population living in retirement communities in the South (40%), with New Orleans alone reporting 23% of adults with a disability (Kraus et al. 2018, p. 8).

The disproportionate impact of disasters on people with disabilities and seniors is heavily documented as recently evidenced after Hurricane Katrina hit the Gulf Coast in 2005 and from past disasters such as Hurricane Andrew in 1992 and the major hurricanes of 2004 that impacted Florida. Of the estimated 1,800 persons who died in Hurricane Katrina and its aftermath, 71% of the victims were older than 60, and 47% over the age of 75. Of the elderly affected by Katrina, most lived independently, and many were disabled and mobility-restricted (Cahalan and Renne 2007; Davis et al. 2009). Supporting this finding, of the 144 total deaths caused by the four major

hurricanes that hit Florida in 2004, 40–60% were persons over the age of 60 (Cahalan and Renne 2007). Studies have attributed increased vulnerabilities (disabled and seniors) to disasters primarily to impaired physical mobility, diminished sensory awareness, preexisting health conditions, and social and economic constraints. According to Phillips, "Higher injury and death rates occur because seniors are less likely to hear warnings, are less able to evacuate effectively or are reluctant to leave their homes, or because they live alone and have few sources of support for evacuation" (Phillips and Morrow 2007, p. 1). She further states, "During response and recovery, the elderly is less likely to use federal programs because they find the rules and regulations of federal bureaucracy to be confusing and a burden" (Phillips and Morrow 2007, p. 1).

Poor planning with and for the disability and aging population also contributes to increased vulnerability during a disaster response and recovery phase. This lack of comprehensive planning further leaves people with disabilities at risk and with fewer options.

Persons with Medical Conditions

Many people throughout the United States may have one or more existing medical conditions, some more severe than others. (If a person with a medical condition becomes debilitated, limited, or otherwise impaired, that person with the medical condition may be protected under the ADA.) Some medical conditions are also defined as a disability and therefore those persons are considered a protected class. For example, people with psychiatric disabilities are included in the ADA definition of "cognitive disability" and are protected under the ADA. However, a person who is deaf may or may not identify him/herself as someone who has a "medical condition," but they are still protected under the ADA.

Examples of medical conditions include people with cancer, Alzheimer's, kidney disease, multiple sclerosis, diabetes, HIV/AIDS, etc. Caring for people with medical conditions is critical during the recovery period and often an aspect overlooked. If medical infrastructure is not maximally functioning during the recovery process, some people with medical conditions may either suffer or not be able to return home. For example, if an evacuee depends on dialysis treatment several times a week and the dialysis center is not functional after the disaster, more than likely that person will either have to stay in an alternate care facility or not able to return to home. This can be particularly disconcerting for people are socially and medically dependent on neighborhood services as well as living independently.

Socioeconomic Status and Ethnicity

People with disabilities are more likely to live at or below the poverty level and have limited access to resources. People with disabilities are nearly twice as likely as people without disabilities to have an annual household income of $15,000 or less (Davis 2005). Most live at a "disadvantage" prior to a disaster, making the effects of the disaster devastating. According to the World Bank, "Poverty causes disabilities and can furthermore lead to secondary disabilities for those individuals who are already disabled, as a result of the poor living conditions, health endangering employment, malnutrition, poor access to health care and education opportunities etc. Together, poverty and disability create a vicious circle" (World Bank Poverty and Disability n.d., main web page).

As poverty rates more generally continue to rise in the United States with 58 million workers making less than $15 an hour and considered "working poor," this impacts not only how the emergency management community responds to and supports recovery but is specifically related to people with disabilities. The unfortunate reality is that several people with disabilities are also located in lower economic brackets. There are approximately 53 million people with one or more disabilities living in the United States (Centers for Disease Control 2015). Unemployment rates are higher among people with disabilities with over 65% of working-age adults with disabilities unemployed. Of these working adults, nearly one third earn an income below the poverty level (Fessler 2015; Fontenot et al. 2018). According to the National Council on Disability (NCD),

> [T]he employment rate of working-age people with disabilities remains only half that of people without disabilities (38 percent compared with 78 percent in 2005). The reason is not that people with disabilities do not want to work: Two-thirds of non-employed people with disabilities say they would prefer to be working. (National Council on Disability 2007, p. 8)

People with disabilities who cannot work full time must depend on Social Security Disability Insurance and Supplemental Security Income to support them. Generally, federal benefits are inadequate and do not "provide a living wage, making poverty an inevitability" (Atkins and Guisti 2003, p. 1). As barriers are broken down and disability rights advocated, people with disabilities are living more independent lives and becoming more integrated into communities and workplaces. Almost half of people with a disability (an estimated 24.1 million people) are considered to have a severe disability. For more than a third of individuals with disabilities, assistive technology is essential to being able to take care of themselves at home (Davis 2005). According to Stapleton et al., "Working-age Americans with disabilities are much more likely to live in poverty than other Americans and generally did not share in the economic prosperity of the late 1990s. At the same time, public expenditures to support them are growing at a rate that will be difficult to sustain when the baby boom generation retires and begins to draw Social Security Retirement and Medicare benefits" (Stapleton et al. 2005, p. 1). Still, economic concerns remain as people with disabilities continue to be a marginalized group.

The term "vulnerability" is often used within different contexts. Planners and geographers will look at geographic vulnerability, such as coastal areas and how hurricanes may affect them (Fordham et al. 2013). In addition to geographic, or location-based, vulnerabilities, there are social vulnerabilities. According to Fordham et al. (2013), social vulnerability "arises out of differential social relations among groups in a given society" (p. 4). For example, social vulnerability includes issues such as income disparity, disability, access to health and mental health, cultural and language differences/diversity, race/ethnicity, and gender (Fordham et al. 2013). Along these lines, in this chapter, we will look at "social vulnerabilities" as it is applied to "vulnerable populations." Vulnerable populations may include individuals and communities that experience barriers to services during and after a disaster or major crises. These populations include people living in poverty and working poor, people with disabilities, older people, and refugees and immigrants. Certain ethnic groups have high rates of disability, including African-Americans and Native Americans at 24.3%, as compared to Asian Americans who have the lowest at 16.6% (Fontenot et al. 2018).

It is important that local emergency managers identify the vulnerable populations within their community and engage with them in planning, response, and recovery processes. People who are vulnerable before the disaster or major crisis strikes are more likely, or at higher risk, of mortality and experiencing disruptions as compared to the general population. Lack of resources prior to a disaster is only heightened after a disaster. The term vulnerable populations must be applied at the local level and incorporated into every aspect of emergency management; emergency management must be *inclusive*, not exclusive.

Emergency Management Plans for Disaster

Vulnerable populations are disproportionately affected by disasters often having higher mortality rates and the recovery period being longer and more challenging (David et al. 2011). For example, during Hurricane Sandy, it took twice as long for electricity to be returned to the New York City Public Housing Projects than to adjacent neighborhoods where middle to upper class residents lived. A recent, but tragic example, occurred when Hurricane Maria contributed to the deaths of nearly 3,000 people due to the exceedingly slow response and recovery period efforts (Newkirk 2018). The next sections provide information regarding the four steps of the emergency management plan – preparedness, response, recovery, and mitigation as it relates to vulnerable and disability populations.

Preparedness

Emergency management preparedness focuses on how local, state, and federal agencies and organizations can prepare themselves for various disasters. The process of preparedness includes conducting risk assessments, working across agencies and organizations during the planning process, and testing, or exercising, emergency operation plans (Phillips et al. 2017; Bullock and Haddow 2003). According to Bullock and Haddow (2003), preparedness can be defined as, "a state of readiness to respond to a disaster, crisis, or any other kinds of emergency" (p. 115). Emergency preparedness encompasses many activities and levels of preparedness not only for emergency management agencies, but for businesses, service-delivery agencies, hospitals, nursing homes, and the like. Emergency managers, who are tasked with putting emergency operations plans (EOPs) together, should consider forming task forces or working groups to ensure all populations within the community are a part of the planning process.

When working with people with disabilities in the planning and preparedness phases, it is critical that emergency managers consult and work directly with the disability community to ensure that no one is left behind. The disability community is not homogeneous, but rather a diverse segment of the US population that should be included in the planning and preparedness phase of emergency management (Davis et al. 2007). All emergency management municipalities are obligated to ensure accommodations under the Americans with Disabilities Act of 1990 (Davis et al. 2007). Given this requirement, it is recommended that disability organizations and agencies be a part of preparedness and planning. In addition, some studies have shown that the elderly is "less likely to receive warnings than younger persons" (p. 180) as a result of being more isolated, less linked to social networks, and diminished physical and mental abilities (Peek 2013).

Emergency managers need to consider the specific language and cultural needs of the refugee and immigrant community within their locale. Ensuring that networks exist to help disseminate information to the immigrant population can be the difference between life and death. Housing advocacy, homeless agencies and shelters, social services, and community centers should be included in the emergency planning process. Of critical importance is ensuring plans include sheltering and temporary and permanent housing.

Response

The response phase is the critical time period when first responders, emergency managers, and crisis human services workers work diligently in a coordinated effort to provide efficient and effective services during a major crisis or disaster (Phillips et al. 2017). Response may include running shelters, evacuations, emergency room activities, and fire and rescue. Disasters pose specific threats to vulnerable populations as at times they have been left behind or lack access to services that sustain their life.

While some people with disabilities live fully engaged and vibrant lives in the United States, during a disaster or major crisis, their ability to evacuate, sustain life without live-saving equipment, or to process the rapid changes and dangers may be significantly diminished. First responders, emergency managers, and crisis human services workers need to be aware of this potential hazard and be prepared to provide, for example, transportation to a shelter that is accessible, ensure that there are alternate forms of communication about evacuations and the disaster in general, ensure medical personnel are available to assist with medications and other issues as necessary. Old age is often a primary factor in deaths after a disaster (Peek 2013), as was seen with Hurricane Sandy and Katrina. For example, of the 1,300 people who died from Hurricane Katrina, "67% were at least 65 years or older" (Peek 2013, p. 172). Of the 100 people who died in Superstorm Sandy, close to 50% were 65 years or older (Mapping Hurricane Sandy's Deadly Toll 2013).

At times, people living in poverty, including the working poor, do not readily have access to transportation to evacuate or have the means to provide temporary housing during a disaster.

When the World Trade Center towers came down, more than 2,700 people were killed (September 11 Fast Facts 2018). While accurate numbers remain unknown, it is estimated that

there were 100 undocumented workers who also perished that day. Perhaps out of fear or lack of access to language-appropriate materials, the families and loved ones of those workers who were killed did not come forward; nor did officials seek them out (Ruiz 2016). Fear, language barriers, or lack of outreach can prevent individuals from not only being counted but receiving post-disaster services that can help them recover.

Recovery

Recovery is considered the longest stage, or phase, of emergency management. Depending on the type, size, and severity of the disaster, the recovery phase can last anywhere from a few days or weeks to years. Human service organizations and agencies, community and civic associations, and human services departments within emergency management play a critical role in recovery. While communities may never be the same after a disaster, there is always an opportunity to strengthen communities and better prepare them for the next major crisis or disaster. According to Phillips et al. (2017), "After a disaster, we must think about a wide array of concerns that face families, communities, organizations, leaders and managers. Recovery, while daunting, provides an opportunity for these kinds of people and the places that they love" (p. 254).

Housing for some people with disabilities after homes are lost in a disaster is paramount. For example, people who use wheelchairs will need new housing that is retrofitted so they can move about independently. For others, loss of paratransit access prevents them from going to their jobs or even to obtain medical care, such as dialysis. For older people, the risk of not being able to access life-enhancing and/or life-saving medications and services is not the only significant disruption. Older people are also at higher risk of isolation and increased mental health issues than invulnerable people.

Housing post-disaster can be especially challenging for people who were living in poverty (i.e., the working poor) in terms of obtaining temporary or new housing, sometimes forcing them instead to return to homes that were heavily damaged. While aid for the federal or state government can eventually support some reconstruction, often there are delays in housing aid programs, long transportation disruptions preventing access to essential daily activities such as work and school, and housing complexes can remain low on overall rebuilding priority lists. In the aftermath of disaster, one type of funding that can be accessed for older people to use during recovery is the Older Americans Act of 1965 (OAA), which provides grants to states for community planning and services. In addition, the OAA is an antidiscrimination law that classifies older Americans as a legally protected class.

Unfortunately, under extreme situations, poverty can put people at higher risk of death as evidenced by the aftermath of Hurricane Maria. According to a research study conducted by George Washington University (2018), "The results of our analysis of total excess mortality by socio-demographic subgroups show that every social stratum and age group was affected by excess mortality. However, the impact differed by age and socioeconomic status. The risk of death was 45% higher and persistent until the end of the study period for populations living in low socioeconomic development municipalities, and older males (65+) experienced continuous elevated risk of death through February" (p. 7).

For non-native English speakers, and people from different cultures or religious backgrounds, the recovery process can be more challenging and isolating, as indicated in the prior section on response. Ensuring safe spaces to receive services and translated materials and interpreters on hand can help dissolve barriers. In addition, working with refugee and immigrant organizations can assist with communication strategies and dissemination of information as well as provide valuable information and resources (Tierney et al. 2001). Often, refugees and immigrants have residual health conditions and mental wellness considerations that are a direct result of their experiences either being forced to flee their homeland (as in the case of refugees) or seeking safety and economic security (as is often the case with immigrants) (Mincin 2017). Emergency management and recovery workers need to be aware of these types of issues in order to appropriately treat them.

Mitigation

According to Bullock and Haddow (2003), mitigation is "a sustained reaction to reduce or eliminate risk to people and property and hazards and their effects" (p. 37). Mitigation is distinguished from the other phases of emergency management because it focuses on long-term efforts at reducing risk (Bullock and Haddow 2003). Preparedness, response, and recovery are focused on how the emergency management and first response community will be ready for, respond to, and recover from disasters. Mileti (1999) explains mitigation as "the policies and activities that will reduce an areas vulnerability to damage from future disasters" (p. 23). In many ways, mitigation includes the concept of community capacity building and resiliency. Working with vulnerable populations before, during, and after disasters offers the opportunity to not only ensure they are *included* in all phases of emergency management and that their specific needs are voiced and met, but to also build stronger, more resilient communities (Tierney et al. 2001).

Universal design is one example that can be considered a mitigation measure for people with disabilities. Universal design refers to ensuring equal access to all people. This may include ramp entrances to buildings, curb cuts on the street, and flashing alarm lights in the hallways of buildings. They are considered universal because the designs both meet the requirements of making things accessible to people with disabilities under the Americans with Disabilities Act of 1990 and can assist people in the "general" or nondisability community. Curb cuts on streets enable people in wheelchairs to move freely about a city or town. It also helps parents and caretakers move children in strollers freely around town. Likewise, flashing fire alarm lights assist people who are deaf know how and when to evacuate a building as well as the "general population." Mitigation strategies can help to reduce death and disproportionate negative effects of disasters on the aging population (Fernandez et al. 2002; Peek 2013). Strategies include shoring up social networks to reduce isolation and increase communication dissemination and ensuring strong infrastructure such as shelters designed for assisting older people (Fernandez et al. 2002).

Mitigation projects for lower-income communities may include strengthening structural aspects such as buildings, electrical grids, and community organizations. Mitigation efforts for the refugee and immigrant communities can include conducting assessments with the help of refugee and immigrant organizations so that education and networks can be put in place. Communities can become stronger and more resilient by seeking to better integrate refugee and immigrant people in their towns and cities.

Conclusion

This chapter provides an overview of how people with disabilities and vulnerable populations might be affected during and after a disaster. Understanding the preexisting conditions such as poverty, disability, and language barriers can assist greatly when responding to and recovering from disasters. In addition, emergency managers can and should reach out to local community, advocacy, and service-delivery organizations and include them in emergency planning, drills, and exercises. These individuals and organizations know the issues and needs of specific populations and can play a significant role in the well-being of your community when disaster does strike. Although not all vulnerable populations are always legally protected, such as people living in poverty, it is critical for emergency managers to robustly include these populations in all phases of emergency management to mitigate loss of life and facilitate speedy recovery. Further, people with disabilities and the aging are legally protected classes and must be incorporated into all phase of emergency management planning and response. People with disabilities and functional needs as well as other vulnerable populations are at increased risk for long-term recovery disruptions and higher rates of mortality during and after disasters. Finally, emergency managers need to ensure accessibility during and after a disaster. Often lack of accessibility unnecessarily creates increased dependence. For example, someone

maybe in a wheelchair and function fine regarding daily living. However, during and after a disaster, maybe become dependent because disaster assistance centers and/or shelters are not accessible. Inclusion is the key to ensuring vulnerable populations are safe during disasters and recover well after the disaster.

Cross-References

- Emergency Management: Crisis Communication
- Emergency Management: Crisis Management and Response
- Emergency Management: Evacuations
- Emergency Management: Infant and Young Children Feeding in Emergencies
- Emergency Management: International
- Emergency Management: Pets
- Emergency Management: Preparedness and Planning
- Emergency Management: Recovery

References

A Guide to Disability Rights Law. (2009). United States Department of Justice. Retrieved from https://www.ada.gov/cguide.htm

Atkins, D., & Guisti, C. (2003). The Confluence of Poverty and Disability. Retrieved from http://www.housingforall.org/rop0304%20poverty%20and%20disability.pdf

Braithwaite, J., & Mont, D. (2009). Disability and poverty: A survey of World Bank Poverty Assessments and implications. ALTER, *European Journal of Disability Research 3*, 219–232. Retrieved from http://siteresources.worldbank.org/DISABILITY/Resources/280658-1172608138489/WBPovertyAssessments.pdf

Bullock, J. A., & Haddow, G. D. (2003). *Introduction to emergency management*. Burlington: Butterworth-Heineman, Elsiever Science.

Cahalan, C., & Renne, J., (2007). Safeguarding Independent Living: Emergency Evacuation of the Elderly and Disabled. *Intransition*, Spring p. 7–12, 29–32.

Centers for Disease Control. (2015). CDC: 53 million adults in the US live with a disability. Centers for Disease Control and Prevention. Retrieved from https://www.cdc.gov/media/releases/2015/p0730-US-disability.html

Cohn, D. (2017). 5 key facts about U.S. lawful immigrants. Pew Research Center. Retrieved from http://www.pewresearch.org/fact-tank/2017/08/03/5-key-facts-about-u-s-lawful-immigrants/

David, E. A., Hansen, R., & Mincin, J. (2011). Chapter 19: Vulnerable populations and public health preparedness. In M. J. Reilly & D. S. Markenson (Eds.), *Healthcare emergency management: Principles and practice*. Sudbury: Jones and Bartlett Learning.

Davis, E. A. (2005). Guide on the special needs of people with disabilities for emergency managers, planners, and responders. National Organization on Disability: Washington, D.C. Retrieved from http://eadassociates.com/epiguide2005.pdf

Davis, E., & Sutherland, D. (2005). It's the law: Preparedness and people with disabilities. *International Association of Emergency Managers Bulletin, 22*(3), 13–14.

Davis, E. A., Hansen, R., & Mincin, J. (2007). *Tools and tips for special needs preparedness planning: Special needs toolkit*. Illinois Public Health Association; EAD & Associates, LLC.

Davis, E. A., Nancy Houston, N., Leckner, M., Mincin, J., Phillips B. D., & Vann Easton, A. (2009 April). Routes to Effective Evacuation Planning Primer Series: Evacuating Populations with Special Needs U.S. Department of Transportation Federal Highway Administration Office of Operations. Retrieved from https://ops.fhwa.dot.gov/publications/fhwahop09022/fhwahop09022.pdf

Federal Emergency Management Agency, Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters. (2010). Retrieved on 12 Mar 2019 from https://www.fema.gov/pdf/about/odic/fnss_guidance.pdf

Fernandez, L. S., Byard, D., Lin, C. C., Benson, S., & Barbera, J. A. (2002). Frail elderly as disaster victims: Emergency management strategies. *Prehospital and Disaster Medicine, 17*(2), 67–74. Retrieved from https://pdfs.semanticscholar.org/da42/be12122f757778ca99179fb3ba9f6761efed.pdf

Fessler, P. (2015 July 23). Why disability and poverty still go hand in hand: 25 years after landmark law. NPR All Things Considered. Retrieved from https://www.npr.org/sections/health-shots/2015/07/23/424990474/why-disability-and-poverty-still-go-hand-in-hand-25-years-after-landmark-law

Fontenot, K., Semega, J., & Kollar, M. (2018 September 12). Income and Poverty in the United States: 2017. United States Census Bureau Report number P60–263. Retrieved from https://www.census.gov/content/dam/Census/library/publications/2018/demo/p60-263.pdf

Fordham, M., Lovekamp, W. E., Thomas, D. S. K., & Phillips, B. D. (2013). Chapter 1: Understanding social vulnerability. In W. E. Lovekamp, D. S. K. Thomas, B. D. Phillips, & A. Fothergill (Eds.), *Social vulnerability to disasters* (2nd ed.). Boca Raton: CRC Press, Taylor & Francis Group.

George Washington University. (2018, August 28). Recommendations aimed at preparing Puerto Rico for hurricane season. *ScienceDaily*. Retrieved 11 Mar 2019, from www.sciencedaily.com/releases/2018/08/180828121419.htm

George Washington University Milken Institute School of Public Health. (2018). Ascertainment of the estimated excess mortality from Hurricane Maria in Puerto Rico. Retrieved on 12 Mar 2019, from https://publichealth.gwu.edu/sites/default/files/downloads/projects/PRstudy/Acertainment%20of%20the%20Estimated%20Excess%20Mortality%20from%20Hurricane%20Maria%20in%20Puerto%20Rico.pdf

Kailes, J. (2008). Southern California wildfires after action report, prepared in partnership with the Access to Readiness Coalition, The California Foundation for Independent Living Centers, and The Center for Disability Issues and the Health Professions at Western University of Health Sciences.

Kailes, J., & Enders, A. (2006). *Moving Beyond Special Needs: A Function Based Framework for Emergency Management and Planning*. Retrieved from http://disability.law.uiowa.edu/dpn_hi/380.pdf

Kraus, L., Lauer, E., Coleman, R., & Houtenville, A. (2018). *2017 Disability Statistics Annual Report*. Durham, NH: University of New Hampshire.

Lopez, G., & Bialik, K. (2017). *Key findings about U.-S. immigrants*. Washington, DC: Pew Research Center. Retrieved from http://www.pewresearch.org/fact-tank/2017/05/03/key-findings-about-u-s-immigrants/

Mapping Hurricane Sandy's Deadly Toll. (2013). Published on November 17, 2012 by New York Times. Retrieved from https://archive.nytimes.com/www.nytimes.com/interactive/2012/11/17/nyregion/hurricane-sandy-map.html

Mileti, D. (1999). *Disasters by design: A reassessment of natural hazards in the United States*. Washington, DC: Joseph Henry Press.

Mincin, J. (2017). Chapter 11: Best practices for refugee resettlement services. In B. D. Phillips, D. M. Neal, & G. R. Webb (Eds.), *Introduction to emergency management* (2nd ed.). Boca Raton: CRC Press, Taylor & Francis Group.

National Council on Disability NCD Report: Empowerment for Americans with Disabilities: Breaking Barriers to Careers and Full Employment, 2007. National Center for Accessible Media (NCAM). Access to Emergency Alerts for People with Disabilities. Retrieved from https://www.ncd.gov/rawmedia_repository/d87db786_9053_49c2_8032_092dddde6752.pdf

Newkirk, V. R. (2018, August 28). A year after Hurricane Maria, Puerto Rico finally knows how many people died. *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2018/08/puerto-rico-death-toll-hurricane-maria/568822/

Peek, L. (2013). Chapter 7, Age. In *Social vulnerability to disasters* (2nd ed.). Boca Raton: CRC Press, Taylor & Francis Group.

Phillips, B. D., & Morrow B. H. (2007). Social science research needs: Focus on vulnerable populations, forecasting, and warnings. *Natural Hazards Review, 8*(3), 61–68.

Phillips, B. D., Neal, D. M., & Webb, G. R. (Eds.). (2017). *Introduction to emergency management*. Boca Raton: CRC Press, Taylor & Francis Group.

Ruiz, A. (2016). Op-Ed: Remembering the immigrants killed on 9/11. Published on September 12, 2016, *Al Dia*. Retrieved from http://aldianews.com/articles/opinion/op-ed-remembering-immigrants-killed-911/44020

September 11 Fast Facts. (2018). Published on August 8, 2018 on CNN Library. Retrieved from https://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/index.html

Stapleton, D. C., O'Day, B., Livermore, G. A., & Imparato, A. J. (2005). *Dismantling the poverty trap: Disability policy for the 21st century*. Ithaca: Rehabilitation Research and Training Center for Economic Research on Employment Policy for Persons with Disabilities, Cornell University. http://digitalcommons.ilr.cornell.edu/edicollect/124.

The World Bank. (2017). Population, female (% of total), World Bank staff estimates based on age/sex distributions of United Nations Population Division's World Population Prospects: 2017 revision. Retrieved from https://data.worldbank.org/indicator/SP.POP.TOTL.FE.ZS

The World Bank. (n.d.). *Poverty and disability*. Retrieved on 12 Mar 2019 from http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTSOCIALPROTECTION/EXTDISABILITY/0,,contentMDK:20193783~menuPK:419389~pagePK:148956~piPK:216618~theSitePK:282699,00.html

Tierney, K. J., Lindell, M. K., & Perry, R. W. (2001). *Facing the unexpected: Disaster preparedness and response in the United States*. Washington, DC: Joseph Henry Press.

United States Census Bureau. (2017). Facts for features: Older Americans month: May 2017. Retrieved from https://www.census.gov/newsroom/facts-for-features/2017/cb17-ff08.html

World Report on Disability (2011), p. xl (see PDF: https://www.unicef.org/protection/World_report_on_disability_eng.pdf

World Report on Disability. (2017). UNICEF. Retrieved from https://www.unicef.org/protection/World_report_on_disability_eng.pdf

Further Reading

Disability and Aging

Disaster Planning Often Leaves Disabled People Behind: https://tonic.vice.com/en_us/article/paw4gk/disaster-planning-often-leaves-disabled-people-behind

Guidance on Planning for Functional Needs and Support Services in General Population Shelters: https://www.fema.gov/pdf/about/odic/fnss_guidance.pdf

Nobody Left Behind: http://www2.ku.edu/~rrtcpbs/findings/ and http://www2.ku.edu/~rrtcpbs/findings/pdfs/bestpractices_3-21-072.pdf

No One Left Behind: Including Older Adults and People with Disabilities in Emergency Planning: https://acl.gov/news-and-events/acl-blog/no-one-left-behind-including-older-adults-and-people-disabilities

Socioeconomic Factors in Disaster

How Disasters Affect People of Low Socioeconomic Status: https://www.samhsa.gov/sites/default/files/programs_campaigns/dtac/srb-low-ses.pdf

Socioeconomic Vulnerability to Disaster Risk: A Case Study of Flood and Drought Impact in a Rural Sri Lankan Community: https://www.sciencedirect.com/science/article/pii/S092180091731604X

Refugees and Immigrants

Addressing the Needs of Immigrants in Response to Natural and Humanmade Disasters: https://www.apha.org/policies-and-advocacy/public-health-policy-statements/policy-database/2014/07/23/17/36/addressing-the-needs-of-immigrants-in-response-to-natural-and-humanmade-disasters-in-the-us

The Impact of Natural Disasters on Immigrants and Refugees in the United States: https://www.gcir.org/resources/impact-natural-disasters-immigrants-and-refugees-united-states-what-funders-need-know

When Disaster Strikes: Responding to Migrants Caught in Crisis: https://www.migrationpolicy.org/article/when-disaster-strikes-responding-migrants-caught-crises

Social Vulnerability

Chapter 1: Understanding social vulnerability (Fordham et al., 2–13) in Social vulnerabilities to disaster, 2nd Ed.

Disaster Risk – Poverty and Inequality: https://www.preventionweb.net/risk/poverty-inequality

Disaster Risk – Vulnerability: https://www.preventionweb.net/risk/vulnerability

EU Private Security Regulation

Spyridon Triantafyllou
John Jay College of Criminal Justice, New York, NY, USA

Keywords

Private security · Security industry · Regulation · EU

Definition

Legislative act to harmonize private security industry across the European Union.

Introduction

The European Union (EU) law is divided into "primary" and "secondary" legislation. The treaties (primary legislation) are the basis for all EU action. Secondary legislation – which includes regulations, directives, and decisions – are derived from the principles and objectives set out in the treaties. A "regulation" is a binding legislative act that must be applied in its entirety across the EU. A "directive" is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals (European Commission).

To date, there is not such legislative act regulating the private security industry meaning that there is no harmonization of the industry of all the EU member states, apart from certain security services which are partially regulated. For instance, the Regulation (EC) 300/2008 has established rules in the field of civil aviation security aimed at protecting persons and goods from unlawful interference with civil aircraft (European Commission).

However, regulation is necessary because private security employees across the EU should act with professionalism and high-level standards. The critical issues for regulation might be synopsized in the following: age, experience requirements, licensure, personal character, and education and training needed (Nemeth 2012).

Why Regulate?

The private security industry is a very diverse industry encompassing a variety of products and services. Private security personnel are not like ordinary citizens, while many security-related occupancies draw upon special privileges (i.e., detainment of shoplifters, use of force by door supervisors, armed by security guards in cash-in-transit vehicles, access to information which might be exploited or abused). If minimum standards are taken away, there is a temptation to lower standards to win business with all the

potential implications that has a poorer quality security sector (Prenzler 2012).

Regulation of private security industry in the EU is of the utmost importance on the political agenda. On the one hand, it is essential to regulate and improve professional standards given the increased needs of public police force, the increased risk of terrorism, and the mundane problems of crime prevention and policing, assuming the overall low standards and widespread problems (Button 2007).

On the other hand, regulation is an important factor for optimizing security, as it needs to adapt and be responsive to meet the changes in the industry, but it should also face the regular challenge of balancing consumer, industry, and public interests (Prenzler 2012). Besides, regulation must be tailored to enhancing private security and not hindering or smothering it, which can occur (Button and Stiernstedt 2018). Consequently, the main question about private security industry in the EU might be synopsized as: do we need *regulation, deregulation, or reregulation?*

The Landscape of Private Security in the EU

A recent motion for action of the European Parliament highlights the value of regulating the private security industry. Specifically, it is mentioned that "*(. . .)* D. more than 1.5 million private security contractors were employed in around 40,000 private security companies (PSCs) in Europe in 2013; *(. . .)* the turnover of these companies in that year amounted to around EUR 35 billion; *(. . .)* K. a legal framework with binding regulatory and monitoring mechanisms should be put in place at international level to regulate their use and provide sufficient control over their activities; *(. . .)* whereas the current regulatory situation in this sector comprises a series of inconsistent rules which vary enormously between the Member States; *(. . .)* P. the European Union does not have a regulatory framework of its own, *(. . .)* Q. whereas it is of vital importance to prioritize the establishment of clear rules for interaction, cooperation and assistance between law enforcement and private security companies; *(. . .)*" (European Parliament 2017).

Several reports and papers underline the dizzying and complex variety of standards relative to regulation by citing the statutory laws of several member states or other statistics and thus conclude the lack of uniformity of standards EU wide (Button and Stiernstedt 2018). Identifying the level of analysis is crucial when discussing the standards relative to regulation in general.

Focusing on the European Union, discussion is expected to deal with national and supranational levels of governance. One of the most important aspects of private security regulation is that instead of protesting about state regulation – as most commercial sectors do – many sections of the private security industry have actively welcomed state regulation (White 2010). Furthermore, regulation has become a way of increasing the presence of state structures in the security marketplace so as to render private security services more "state-like" (Smith and White 2014). But the scope of this analysis is limited to the EU context, despite the fact that regulatory issues about standards of private security system are mainly addressed by the member states.

According to rulings of European Court of Justice, the private security industry is considered an economic sector of the EU and, therefore, falls under the regulation of the internal market (Born et al. 2007). There are also other issues that may affect further regulation of private security industry in the EU while at the same time making imperative the need for adopting a new EU private security regulation.

According to Directive 2006/126/EC, security services are considered just another services in the open market, notwithstanding the particularity of the industry as mentioned above. This essentially means that from the supranational point of view, the private security companies will never be fully able to function in transnational level without disastrous consequences for the standards of the industry, since there is not a homogenous field in European level setting minimum standards for their action. Besides, the question of sovereignty does impact on the tendency for more integration of the private security industry. Again, an attempt

to harmonize this field should be welcomed as means to raise the standards of the industry EU wide (Loxa and Siagkou 2016).

Finally, assessing the Europeanization of the industry, three dimensions should be taken into consideration: (a) the possible *market failures*, affecting the trustworthiness of the sector and hampering efficient private-public collaboration strategies (i.e., the existence of false independent contractors, unfair dumping of prices, high competition can create a dysfunctional balance between supply and demand of security services), while an antidote for the regulatory power of the single market might be European Quality Standards; (b) the *creation of EU minimum guidelines* regarding private security across the EU member states is directly aimed with legislation (i.e., requirements for training, licensure, control); and (c) rethinking *European or international collaboration strategies*, emphasizing on the fact that the private security sector must strengthen its ties with European institutions (Pashley and Cools 2012).

Pertinent to this contribution are the following documents: the "Handbook State Regulation Concerning the Civilian Private Security Services and their Contribution to Crime Prevention and Community Safety" (UNODC 2014), the "Private Security Services in Europe Facts & Figures" (CoESS 2011), and the "Security regulation, conformity assessment and certification" report for European Commission (ECORYS 2011) (*see* Further Readings).

Conclusion

The rise of private security industry across the European Union and the different level of industry regulation in each and every Member-State have made imperative the adoption of an EU regulation. However, such legislation has not passed yet, despite any political implications and the increasing size and needs of the industry in the context of single market. Some initiatives on behalf of EU organs have already mentioned reflecting the importance and the potential of private security to the overall security of the EU. It remains to prove that the in-name-only "EU Private Security Regulation" will actually become a reality across the Union and not remain merely pious hope.

Cross-References

- ▶ EU Private Security Regulation
- ▶ Mercenary and Private Military
- ▶ Public-Private Partnerships: Security Organizations
- ▶ Public-Private Partnerships: Training and Coordination in Disasters
- ▶ Security: Private

References

Born, H., Caparini, M., & Cole, E. (2007). Regulating private security in Europe: Status and prospects. *The Geneva Centre for the Democratic Control of Armed Forces (DCAF)*, Policy Paper 20.

Button, M. (2007). Assessing the regulation of private security across Europe. *European Journal of Criminology, 4*, 109–128.

Button, M., & Stiernstedt, P. (2018). Comparing private security regulation in the European Union. *Policing and Society, 28*(4), 398–414.

European Parliament. (2017). Report on private security companies, *Committee on Foreign Affairs, Rapporteur: Hilde Vautmans*, report 2016/2238 (INI).

Loxa, A., & Siagkou, D. (2016). Private security companies in the EU. In *Lund student EU law review* (Vol. 3, pp. 7–26). www.jur.lu.se/eu_law_review

Nemeth, C. (2012). *Private security and the law* (4th ed.). Waltham: Elsevier Butterworth-Heinemann.

Pashley, V., & Cools, M. (2012). Private security *in* Europe: Towards a European private security model for the future. In M. Cools, B. De Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. V. Walle, T. V. Beken, et al. (Eds.), *European criminal justice and policy* (Vol. 7, pp. 93–114). Antwerp/Apeldoorn: Maklu.

Prenzler, T. (2012). *Policing and security in practice: Challenges and achievements*. New York: Palgrave Macmillan.

Smith, M., & White, A. (2014). The paradox of security regulation: Public protection versus normative legitimation. *Policy and Politics, 42*(3), 421–437.

White, A. (2010). *The politics of private security: Regulation, reform and re-legitimation*. New York: Palgrave Macmillan.

Further Reading

Confederation of European Security Services (CoESS). (2011). *Private security services in Europe*

confederation of European security services facts & figures. Brussels: CoESS Secretariat.
ECORYS. (2011). *Security regulation, conformity assessment and certification. Final report (1)*. Brussels: European Commission, DG Enterprise and Industry.
United Nations Office on Drugs and Crime (UNODC). (2014). State regulation concerning civilian private security services and their contribution to crime prevention and community safety. In *Criminal justice handbook series*. Vienna: United Nations Office.

Event Security

Mark Camillo
Security, Fire and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Celebratory event security · Commemorative event security · Diplomatic event security · Entertainment event security · Festival event security · Mass gathering event security · Religious event security · Special event security · Sporting event security

Definition

For the purposes of this unit, event security can be defined as the plans, design, and implementation of measures required to create and maintain a safe environment for a planned event that includes attendance and participation of a private or public nature.

Introduction

Physically securing events is not a new phenomenon; however, over the past 20 years (1998–2018), the globally accepted approach has evolved into a methodology where all hazards of a reasonable nature are factored into the security plan. This topic will be addressed in a manner that allows the reader to gain an understanding of the potential risks which could cause a disruption to an event, how securing an event should be accomplished, and the potential consequences event security managers much consider, such as postponing the event to experiencing a crisis where death and/or serious physical injury to those on site is likely to occur.

Types of Events

Events that warrant securing have historically fallen in several categories that include but are not limited to:

- Entertainment (e.g., music festivals, concerts, and parades)
- Ceremonial (e.g., college graduation commencement)
- Sporting (e.g., Olympics, FIFA World Cup)
- Faith-based (e.g., the Hajj to Mecca)
- Diplomatic (e.g., G7 Economic Summit, US Presidential Inauguration)

Events such as the examples listed above are not unique to one particular country or culture. These events are generally social in nature, with an announced time and place. The size of attendance is often driven by the type of event. For example, a college graduation commencement may take place depending on the size of the graduating class and audience scheduled to participate and attend, respectively. Similarly, an entertainment event may take place at a venue considered large enough to appropriately host the anticipated patrons. Sporting events such as golf require an approach different than a stadium due to the expansive nature of the area where the competition takes place. No single approach to securing an event can be duplicated without tailoring it the unique nature of the event. Many security components do have general application; however a review of previous security plans for similar events is recommended to compare and adopt or dismiss based on any unique needs of the upcoming event.

Event Venue Nomenclature

Back of the House (BOH)

This term is likely sourced to eating establishments and performing arts venues. The "back of the house" (BOH) is often referred to the areas where workers, talent, equipment, product, etc. are entering or produced in the venue. General public or ticketed public do not normally enter the venue from back of the house entrances. This is an important reference term to remember when creating an event security plan.

Front of the House (FOH)

This term is applied to where the public or invited guests enter the venue during scheduled event times. The front of the house (FOH) is where crowds both enter and exit an event unless event operations open additional exits at the conclusion of an event.

Building an Event Security Plan

Risk Determination

Threats Versus Hazards

It is very important to distinguish how an event may be of risk. A threat is generally understood to be of a man-made nature, where a hazard is a result of a natural occurrence (e.g., blizzard, earthquake, wildfire, and flooding). Both threats and hazards must be factored into the design and development of a security operation.

> Many security professionals and their clients confuse threats and hazards. Hazards can be either natural or man-made and are generally unintentional or without malice. Threats are always man-made and intentional and with malice. (Norman 2016, p. 111).

Threats may be detected and deterred through preventative countermeasures. Natural hazards such as severe weather are not likely preventable, but mitigation measures and emergency response protocols can be put in place in advance to lessen the chances of damage to property or personal physical injury. Regardless of the potential danger that has been identified, the level of risk must be predetermined in order to effectively mitigate hazards or counter threats.

Before determining the degree of risk faced by an event, assessing the contributing factors that will constitute the risk is prudent. Today's security professional understands the importance of conducting a risk assessment of an event and the environment of which it will take place. When conducting the initial assessment, it is recommended that all physical vulnerabilities be identified.

Vulnerabilities

Vulnerabilities would be simply described as where "gaps" are identified in the perimeter that threat actors might exploit the operational environment. Access points that are controlled both on event day and nonevent day are considered positive elements to securing a venue. Due to spectators or attendees that arrive on event day prior to the scheduled event, gates or predetermined entrances for crowd access must be critically examined for placement of security personnel and equipment. Due to the spectrum of security measures that may be deployed at events, these access areas must be able to accommodate the security screening and ticket-taking if they are co-located. All perimeter fencing must be examined to ensure it is intact and is of the correct design, height, and strength to deter a threat actor or unauthorized person from accessing the event. A strong event security plan can only be achieved with prevention and protection measures in place. The vulnerability assessment should identify all weak areas to be addressed before the event.

> After fully understanding the operating environment, note any physical security vulnerabilities that could be exploited by threat actors in this operating environment. These may include unintended access points; abuse of normal access points by stealth, trickery, or intimidation; and types of assets any threat actor might be interested in. (Norman 2016, p. 93).

Threats

In addition to a vulnerability assessment, a threat assessment must also be conducted to determine any negative interest a person or group might direct toward the event. This includes their threat vector

or path and tools used in the attack. Threats may emanate from groups or individuals. Intuitively, threats are likely to originate from outside an event venue, but a comprehensive threat assessment must include the "insider threat." This type of threat actor may be already employed by the venue or a company under contract to provide services to the venue and/or event. Many companies are brought together, particularly in sporting and entertainment events, to bring the event to a successful conclusion. Not requiring "in-house" organizations and contracted organizations to conduct background checks on their employees before working an event creates a porous threat environment. The overall "workforce" at an event must be factored into the threat picture. Outside threats can source from hate groups, criminal enterprises, and extremist groups to name a few.

Consequences

The final area to factor into a risk assessment of an event is the consequences, or negative impact of an incident. Prominent examples would be the devastating effects caused by natural disasters. In the context of analyzing risk for events, this would include severe weather. Outdoor events in particular such as sporting competitions and parades can sustain considerable property damage and potential injuries to participants and attendees if the consequences of a severe weather event are not factored into the overall risk mitigation plan.

> Weather should factor in your risk assessment, and you should come up with contingency plans for your various 'what if' scenarios. For example, you might be hosting a celebrity golf tournament that will attract thousands of visitors. What contingency plans must you have in place if there is a sudden violent thunderstorm with hundreds of spectators seeking cover from lightning strikes under the trees? You must have the capability of being alerted in good time of approaching storms, and all stewards must be fully aware of what action to take should the need to evacuate the course arise. (Walton and Philpott 2011, p. 10).

Capabilities Determination

The fundamental needs in achieving an effective event security operation require addressing requirements in the areas of people, process, and technology. In a perfect scenario, the event security planner would have access to skilled personnel and a variety of physical security countermeasures. Essential training of personnel would not be an issue and would include skill development in areas such as:

- Patron screening equipment operation and techniques
- Bag search techniques
- Hostile surveillance detection

The cost of equipment would also not affect the overall budget of the operational security plan. All elements in place would be driven by a seamless process that ensures operational readiness. This is of course not reality.

Event security is unique in that crowd flow and the amount of time allotted for admittance before an event will drive the design of screening at entrances and the items permitted into the event. It is important to clearly understand any limitations placed on entering patrons by the event organizer or host venue. Prohibited items posted on signage outside the venue and on the event website have proven very effective in reducing the number of prohibited items identified by screeners at the entrance gates. An example would be liquids. Some events allow bottled water, while other events do not allow any liquids unless for medical/health purposes. Limiting items and the size of bags entering an event may reduce baggage screening to visual searches by event security personnel. This is, however, not as effective as a bag of any size being searched by a trained event security screener.

Event Access Control

Those responsible for determining the level of access control effectively control the event. Planned and/or scheduled events are well-advised to implement ticketing for access during the scheduled event. Internal areas require credentials to provide access for authorized individuals who are permitted to enter restricted areas. Credentials are issued to various groups to include workers, special guests, and entertainment groups.

Credentials do not supersede the physical screening measures outlined below. Everyone entering a venue whether they are spectators or engaged in a working capacity must be screened to ensure consistent protective measures are in place at the venue.

Ticketing and Invitations

Events with no restriction regarding who is allowed to enter can be conceptualized as having a host of potential issues. Among the top concerns would be the inability to determine in advance the amount of space required to safely assemble the attending crowd. This creates challenges especially for both event security providers and public safety entities who develop their deployment plan of personnel and equipment based on projected crowd size. A ticketed event or event that restricts attendance to a predetermined guest list allows for a properly staffed and equipped event security operation.

Patron Screening

This is a critical component in an event security operation. Whether the term used is patrons, attendees, or spectators, the front of the house at the venue is where patrons should be screened at the level determined by the venue or the affected authorities. Generally, sporting leagues have recommended best practices that include the level and types of screening. The type of event may drive the level of patron screening. Some venues maintain a consistent level of screening regardless of the event. Screening equipment and techniques to consider would be:

- Walk-through metal detectors
- Handheld metal detectors
- Pat-down searches

Patron screening is recommended to be positioned outside the venue if possible or minimally at the venue entrances.

Bag Search Screening

This critical element is dependent on any size or style limitations set forth by the venue or sanctioning body, i.e., sporting league or conference. Tables positioned in immediate proximity to the patron screening operation allow for patrons and their belonging to be checked in a manner that eliminates items to be discretely moved from the patron to the bag or vice versa. Items of an illegal, prohibited, or suspicious nature should be immediately brought to the attention of nearby authorities. It is recommended that bags be visually inspected and, when a questionable item is observed, the patron be requested to remove the item and place it on the table.

Vehicle Screening

Vehicles permitted to enter the back of house delivery areas, i.e., loading dock or adjacent parking lots within the established venue perimeter, would be screened in accordance with the back of the house section of the event security plan. Setback is a term used to describe the distance between public areas and entrances to the venue. A properly designed perimeter plan includes creating as much setback as reasonably possible. Urban-situated venues often have minimal setback due to the dense streetscapes surrounding the venue. Regardless of the setback from public streets and sidewalks, it is recommended that an access control checkpoint be established with anti-ramming technology in place. Vehicle and occupants should be on a preauthorized list in order to enter the venue grounds. The manner in which vehicles are screened should be in accordance with venue-approved improvised explosive device protocols or defer to on-site public safety personnel assigned to perform this function. Optimally, all vehicles such as delivery trucks and team buses should be screened prior to entering the venue. An exception might be team buses coming from a secure location such as an airport. They are generally permitted to enter with a police escort that has ensured the integrity of screened buses.

Event Exterior Concerns

Ingress Crowd Flow

The density of the crowd assembling to enter a security checkpoint can be an inviting target for attack. Threat actors can weave their way into the crowd and achieve their objective using items such as small firearms, improvised explosive devices, or even edged weapons.

Suggested Countermeasures

- Add surveillance detection officers on the exterior out front of the entrances on event day to look for inappropriate or pre-attack behavior.
- Coordinate with your local law enforcement agency to determine if they have officers assigned to detect hostile surveillance or pre-attack behavior.
- Work with both your local law enforcement agency and recommended private security companies to have specially trained K-9 teams that can detect vapors emitted by individuals carrying or wearing explosive materials.

Egress Crowd Flow

Patrons exiting after an event naturally move in mass, thereby creating another crowd density situation. A threat actor only has to "swim upstream" far enough to find the crowd conditions attractive enough to carry out a malicious act, with no intention of entering the building. An example of this type of attack would be the one that occurred in May 2017 at the Manchester Arena, England, following a music concert by American singer Ariana Grande. A suicide bomber detonated a backpack improvised explosive device (IED) in an area outside the arena accessible to the public (Manchester Evening News 2018).

Suggested Countermeasures

- Extend your event security coverage to redeploy personnel outside the venue to ensure any barriers set up to manage the egress are not compromised.
- Coordinate with law enforcement to ensure uniformed officers are positioned at and near the exit points to detect and/or respond to suspicious behavior exhibited by persons observing exiting patrons.
- Extend the assignments of your canine explosive detection teams to be patrolling the periphery of the venue for potential threat actors carrying or wearing explosive devices.
- Ensure that the exterior perimeter plan developed by you and law enforcement extends from your venue to adjacent mass transit stations such as trains or subways.

Ramming Vehicles

As we have sadly seen at recent global events, the determined attacker may resort to driving a vehicle at a high rate of speed into a crowd capitalizing on their vulnerability when outside the venue.

Suggested Countermeasures

- Survey the walkways connecting to your venue to determine if vertical posts known as bollards are positioned in a pattern that prevents a passenger vehicle from accessing the sidewalks from a street. Fixed metal posts are known as traffic bollards, but temporary barriers can also be purchased or leased to fill any gaps. Collapsible or retractable bollards are a good choice for back of the house locations such as loading docks.
- Coordinate with law enforcement counterparts to determine where large vehicles such as trucks or buses may be parked to temporarily block vehicle access on event day.

Artist Security

Entertainers also referred to as the "talent" are susceptible to injuries while performing. Some incidents to consider within the venue would be:

- Accidents or assaults involving talent
  - Artists injured due to slips, trips, and falls
  - Artists grabbed or pushed by patrons
- Stage collapse
- Lack of properly positioned and staffed movable barricades for crowd management

Active Shooter

Properly implemented security countermeasures noted in the Event Access Control section should significantly mitigate the chances of a patron entering into an event site with a firearm. However, at outdoor (open-air) events, an active shooter situation occurring outside the venue is plausible. Targeted areas can include ingress/egress areas at an event site, parking lots adjacent to an event site, or locations at a distance that offer a clear vantage point. This is known as a standoff threat. The mass shooting spree that occurred in October 2017 in Las Vegas, Nevada, during an outdoor music festival exemplifies the possibility of an active shooter targeting concert-goers from a

location that is far from the event site (Las Vegas Strip Shooting 2017). This threat cannot be mitigated without public sector involvement, law enforcement in particular.

Suggested Countermeasures

- Employ hostile surveillance teams at locations outside ingress and egress points of the venue to identify and alert authorities when pre-attack behavior is detected.
- Coordinate with law enforcement counterparts to determine if a counter-sniper plan and assets are in place due to locations at a distance that might offer a shooter to clearly target patrons.
- Offer security personnel to assist law enforcement in posting vantage points of concern for the purpose of observing and reporting the presence of a potential threat actor.

Crowd Behavior

The behavior of a crowd, particularly at music concerts and festivals, should be factored into the overall event security plan. Crowd management must prioritize protecting the crowd from the crowd. Some of the activities and situations to prepare for that are associated with music festivals include:

- Mosh pits (rough physical activity by concert-goers in front stage area) (Mosh Pit Definition 2018)
  - Injuries to concert goers and event staff possible
- Crowd surfing (concert-goers physically passed overhead in a prone position) (Crowd Surfing 2018)
  - Injuries and unwanted touching can be the consequences.
- Intoxication (this has both health and legal implications for intoxicated fans)
  - Arrest for alcohol intoxication and serious physiological reactions possible
- Illicit drug use (combined with alcohol increases chances of overdosing) (Illicit Drugs at Music Festivals 2018)
  - Amnesty boxes are often positioned at screening areas to offer patrons an option of disposing of drugs before being screened or bags searched.
- Crowd density (mass gathering without metering or evacuation measures can escalate if not monitored to conditions with catastrophic consequences) (Love Parade Music Festival 2018)

A complete event security plan has event security staff prepositioned between the performance areas and the crowd as well as in key areas to ensure movement of crowds to reduce crowd density that occurs due to overloading of stage-front viewing areas. Event personnel are often positioned in the "pit area" which is located between a standing crowd of concert-goers and the stage. Security personnel who work in this area during concerts are often referred to as the "pit crew."

The Importance of Collaboration and Coordination

Event security planners cannot create an effective plan in a vacuum. It is imperative that all key stakeholders ranging from venue management to assigned public safety agencies collaborate on the plan. Some may have different objectives, but all share a common goal of having a safe event.

Conclusion

Events, large or small, potentially draw negative attention. Tactics ranging from small-scale attacks to deploying weapons of mass destruction all fall within the threat spectrum. Be ready by being prepared and resourceful. The threat actor only has to get it right once. You must get it right for every event.

Cross-References

- ▶ Criminals: Terrorists
- ▶ Critical Infrastructure: Commercial Facilities Sector
- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats

References

Crowd Surfing. http://www.geeksandbeats.com/2014/06/the-origins-of-crowd-surfing-who-did-it-first/. Accessed 07 May 2018.
Illicit Drugs at Music Festivals. https://www.recovery.org/topics/drug-use-music-festivals/. Accessed 07 May 2018.
Las Vegas Strip Shooting. https://www.washingtonpost.com/graphics/2017/national/las-vegas-shooting/?utm_term=.2ed14f1aea43. Accessed 08 May 2017.
Love Parade Music Festival. https://www.theguardian.com/world/2010/jul/.../love-parade-festival-tunnel-stamped. Accessed 07 May 2018.
Manchester Evening News. https://www.manchestereveningnews.co.uk/news/greater-manchester-news/manchester-arena-terror-attack-19-13075943. Accessed 07 May 2018.
Mosh Pit Definition. https://www.merriam-webster.com/dictionary/mosh%20pit. Accessed 07 May 2018.

Further Reading

Madensen, T., & Knutsson, J. (2011) *Preventing crowd violence* (Crime prevention studies). Boulder: Lynne Rienner Publishers. ISBN-13: 978-1588267535.
Norman, T. L. (2016). *Risk analysis and security countermeasure selection* (2nd ed.). Boca Raton: CRC Press. ISBN: 9781482244205.
Walton, B., & Philpott, D. (2011). *Special event security planning and management*. Longboat Key: Government Training Inc. ISBN-13: 978-1937246792.

Executive Protection

Robert Matthiessen
Security, Fire, and Emergency Management,
John Jay College of Criminal Justice,
City University of New York,
New York, NY, USA

Keywords

Close-protection · Executive protection · Site advance · Motorcade and route management · Formations

Definition

Executive protection is the protection of a human asset against harassment, injury, death, and embarrassment.

Introduction

Executive protection is a specific and unique area of the security industry. It is primarily responsible for safeguarding a person against harassment, injury, death, and even embarrassment. Executive protection is also a highly sensitive security assignment that not only requires the executive protection professional to ensure the safety and security of the executive but to maintain strict confidentiality and professionalism (June, 2008). This chapter describes the basic fundamentals for providing executive protection security for an executive and should be used as a foundation for a structured and comprehensive close-protection security model. Most executives are part of an organizational structure and, as such, require protection because of their senior leadership position and/or affluence. Executive leaders are considered top decision-makers; and if they are incapable to lead or make decisions for their organization, it can affect the executive's reputation, credibility, and even its stock price of the organization. The truth is many executives do not fully understand the role and responsibility of the executive protection professional (EPP). Executives often view the executive protection professional as someone who needs to be available if an emergency or crisis was to occur; however, the executive protection professional is much more than that.

Executive Protection: The Tough Road Ahead

Some executives are apprehensive and do not always appreciate the executive protection professional interfering or monitoring their movements or personal space. While some executives believe that they can take care of themselves without assistance, others may be ridiculed by colleagues for having (and feeling as though they need) security. All of these concerns can have a negative effect, not only on the executive protection professional but on the ability of the executive protection

professional to ensure a safe and secured environment for the executive.

Effective and robust executive protection programs must be developed, analyzed, and implemented based on threats, vulnerability, risk, and a *willingness of the executive to participate in the security program.* This productive approach can identify challenges and obstacles, which must be addressed if an effective and efficient executive protection security program is going to be successful. It can also identify areas that may need additional strategic security planning towards maintaining the highest standard of personal safety and security for the executive (June, 2008).

A primary responsibility of the executive protection professional is to limit the amount of risk exposure to the executive using sound and productive security and risk reduction strategies. The executive protection professional must incorporate all available security functions and methods, while continuously assessing all relevant data relating to all threats, vulnerabilities, and risks. It is critically important that the executive protection professional understand the overall risk analysis and apply security and protection strategies based on the probability of an incident occurring.

The executive protection professional must also be able to maintain an effective level of security, while ensuring a level of "comfort and normalcy" for the executive. Though, this is easier said than done, the executive protection professional must attempt to "strike a balance" between security and the ability of the executive to move freely and not feel hindered or restricted. Many close-protection security personnel fail when beginning their careers because of the assumption that the executive fully understands what personal protection is and how it must be conducted. Unfortunately, many executives utilizing a close-protection professional (same as the executive protection professional) do not understand how protection security should be applied and demonstrated.

Executive protection security has evolved into a more contemporary form of specialized security. It is both an exciting and demanding responsibility within the security industry and will require a commitment of professionalism, diligence, and integrity. The executive protection professional must be highly trained and well-equipped to handle the enormous responsibilities that will be entrusted to them by the executive. It will require extensive and continuous theoretical and technical training, which will be needed to confront the many current threats that executives face around the globe today.

Historically, protection personnel were exclusively chosen for the private sector from federal agencies, such as the United States Secret Service, United States Department of State, the military, and from municipal police departments because of their past training and experience. The advent of commercial close-protection training schools has elevated the civilian population towards filling the ranks of corporate organizations towards addressing their executive protection security needs. Many private organizations now utilize close-protection professionals to perform executive protection services for senior leaders as a preventive mechanism to ensure resilience, asset, and even brand protection (West 2018). The ability to ensure the personal protection of an executive can provide reassurance to a company and its stockholders. This is considered part of a robust and effective protection strategy.

The executive protection professional will continue to provide personal protective security services across a broad spectrum of threats now and in the future. Throughout the decades crime and violence have increased across the globe, to include violence in the workplace. Active shooter incidents, assassinations and attempts, as well as kidnappings have led to injury and death for many executives. These incidents have all contributed to the growing concern and need for specialized professionals trained in protection security. Private organizations have recognized the value of having an executive protection security program as it provides a safe environment for the executive, while reducing the overall risk levels associated with both professional and personal activities (Dale 2008).

The executive protection professional has evolved from a reactionary figure to a proactive and strategic planner. Known as *areas of concentration*, the executive protection professional can develop and implement sound and productive strategic planning for personal protection, motorcade security, site advance, physical security for primary assets, first-aid, counter surveillance, and threat and risk analysis for the executive. The executive protection professional must be proactive in assessing and countering incidents that can hurt or embarrass the executive. This can be difficult to accomplish in all environments, especially when the executive is reluctant to work with the executive protection professional in following the security recommendations.

The main responsibility of the executive protection professional is to remove the executive from the danger zone using a *cover & evacuate (C&E)* method (Dale 2008). The executive protection professional should always focus on prevention and the avoidance of trouble rather than confronting it. An effective executive protection professional providing executive protection security must be able to analyze the environment for potential trouble before it starts. This can be accomplished by experience and the executive protection professional maintaining continuous levels of training in order to remain effective in this role.

Comprehensive security planning is critical for protecting the executive; however, overwhelming the executive with convoluted security models and procedures can equally fail because of frustration on the part of the executive. The executive protection professional must provide a safe environment for the executive that is not intrusive, overwhelming, or hindering as this milieu can result in confusion and possible conflict between the executive and the executive protection professional. This directive can also help in ensuring the security plan is not only approved but embraced by the executive.

Setting a professional standard early on will ensure the executive protection professional and the executive understand what is expected and what is not tolerated. The executive protection professional must be respectful and professional while maintaining the primary role as a protection professional. The executive protection professional must have both hands *free* at all times and remain disciplined as to not violate this important rule. In particular, allowing and accommodating the executive's requests for carrying packages or holding personal items will result in the executive protection professional becoming disengaged, hindered, and not focused (Oatman 2006). The executive protection professional certainly has many challenges ahead, but maintaining professionalism and adhering to the primary principles of close-protection security can result in an effective and efficient program.

Protection Site Advance

Comprehensive and effective site advance is needed to ensure the location the executive is visiting is safe. It requires conducting comprehensive security planning that identifies vulnerable areas at the location. This critical measure is part of a robust executive protection security plan that provides the necessary security and safety steps to stop an attack on the executive; as well as protect the security team.

Advance work also requires the executive protection professional to conduct motorcade route surveys to ensure the quickest and safest way for the executive to get to the location. A threat assessment can help identify dangerous areas in and around the location the executive is visiting. If the location presents security and safety concerns for the executive and the security team, the executive protection professional conducting the site advance must relay that information immediately to the security detail and/or the executive. Effective site advance requires the executive protection professional to arrive at a location at least one hour prior to the executive. Checking for protesters, suspicious individuals, and/or dangerous conditions both outside and inside the site should be performed and corrective action taken. This important responsibility can help in preventing harm or embarrassment to the executive (Oatman 2006).

A checklist is a useful tool, but it must be reviewed continuously, updated, and based on current threats to ensure the executive protection professional is providing a comprehensive and effective security environment for the executive. Site advance checklists are universal and can be found in most close-protection textbooks or other on-line publications. The executive protection professional must also coordinate with host committee staff to verify the activities that will take place when the executive arrives. The executive protection professional can request help from both security and engineering staff at the site to obtain critical information on the location.

The site advance should be outside for the arrival of the motorcade and wait for the executive to exit the vehicle. The advance must now escort the executive and the security detail, if assigned, into the location and directly to their meeting area. When the executive is situated at the location and no ongoing threats or problems exist, the site advance should move to the next location based on the executive's itinerary to conduct the next site advance for the executive.

Protection Intelligence

Protection intelligence requires the gathering of all information either directly or indirectly relating to the executive or the location being visited. This is important because it can help the executive protection professional analyze and formulate an effective security environment towards reducing the overall risk level against the executive and EPP team (USDS 1997). The information can be gathered from direct, open, or paid intelligence sources and can help in the assessment of the overall security planning for the executive. The information should be continuously updated, analyzed, and used to direct the necessary security changes towards addressing all threats and risks. The executive protection professional must conduct regular and comprehensive analysis of all information affecting the executive, make recommendations to the executive regarding security and safety changes, and implement the strategies as needed.

Threat Assessment: Calculating the Risks

A primary tenet of close-protection is conducting a comprehensive threat assessment. An experienced executive protection professional knows it is difficult to determine what level of protection security is needed unless a complete and current threat and risk assessment is conducted. Many close-protections professionals believe that threat assessments as well as risk assessment are universally interchangeable. They are not, and mistakenly applying them can result in increased exposure and/or frustration for the executive. It can also result in increased costs, which will be scrutinized.

A threat assessment will be needed if the executive protection professional wants to successfully develop a comprehensive executive protection security plan. Providing the same level of protection security for all environments can be both dangerous and not very cost effective. The threat assessment can identify potential dangers that the executive and the security team may encounter. This can help towards formulating a more specific security plan for the executive. In any case, when tasked with developing a threat assessment, the executive protection professional must gather as much information as possible on the person(s) who may have an interest, motive, intention, and, more importantly, the capability of mounting an attack on the executive.

Gauging the possibility of a potential threat is critical to the protection of the executive and the executive protection professional (Blankchtein 2013; Holder and Hawley 1998, Kobetz 1991). Mentioned in the *Protective Intelligence* section, the information must include current data and other sources of information pertaining to the executive and his or her family. Analyzing open source information, as well as known threatening communications received, can help in calculating a comprehensive threat assessment. Unfortunately, there is no one descriptive profile of an attacker. Assassins vary by gender, culture, and intelligence. An attacker may engage in familiar behaviors and actions before they attack. These steps have visual characteristics that can be observed by the

executive protection professional. These steps would most likely include acquiring a weapon, surveying security near the executive, and the development of a written attack plan. The executive protection professional must remember that developing a strong and effective threat and risk-assessment plan must also include budgeting and acceptance by the executive who must follow the plan (Dale 2008).

Close-Protection First-Aid

The executive protection professional must be trained in first-aid if the executive is injured or becomes ill. First-aid must be part of a comprehensive executive protection security plan to provide immediate medical treatment in the event of an attack, a medical condition, or an accident. First-aid includes CPR, as well as blunt and penetrating trauma injury response. The executive protection professional must be certified in the first-aid and should be recertified annually. The executive protection professional should be familiar with and know the locations of area hospitals, especially hospitals designated Level-One Trauma centers. The executive protection professional must be familiar with any medicines or medical conditions the executive has to advise emergency room physicians when needed (Dale 2008). Medical conditions, medicines, and other important information pertaining the health of an executive should be known by the executive protection professional. This is especially important for international travel where medical services are limited. The executive protection professional must assess and investigate medical services in countries outside of the USA.

Operational Security and Close Protection Terminology

Close-protection security uses specific terminology to ensure confidentiality and security for the executive, the executive's family, and the security team. Exposing specific addresses, names, and activities can be very detrimental to the executive and the executive protection professional as it can alert a potential attacker where the executive is located, the time of the executive's arrival, and what activity will take. The executive protection professional should utilize "code words" that are changed regularly to ensure that any criminals or potential attackers cannot obtain sensitive information that could help in executing a successful attack, including kidnapping the executive. Operational security also includes strict security measures to safeguard all information on the executive and family members. History has shown that the use of confidential *codes names* can reduce the overall risk level, thus reducing the potential for danger to the executive and the executive protection professional.

Formations: A Tactical Approach to Close-Protection

It is likely that the executive may at some point be the target of an attack, whether by gun, knife, or even a whipped cream pie. If the executive is confronted, injured, or embarrassed, the executive protection professional has already failed. The executive protection professional's ability to perceive and identify danger will be in question and re-training will be needed barring termination.

Tactics are available that the executive protection professional can use to protect the executive. Constant vigilance must be used by the executive protection professional at all times. A primary tactic used for the protection of the executive is known as "*Arms-Reach.*" Situational awareness by the executive protection professional that a gun or other weapon has been produced in the presence of the executive is critical. The primary tactic of the executive protection professional is to "cover" and "evacuate" the executive away from the threat environment. If the attack is from an object that is thrown, i.e., a brick, an egg, or a liquid, the "Arms Reach" method still applies and "cover" and "evacuate" is

needed. The executive protection professional should remove the executive from the area and proceed to a safe room or the motorcade.

Responding to an attack requires information that helps the executive protection professional know where the threat is and which direction the executive protection professional and the executive can evacuate. The use of the *"clock method"* to identify the location of a threat is an effective method used successfully. The 12 o'clock position consists of identifying a fixed object on a wall. If an attack occurs, or a weapon is produced, the executive protection professional using the clock method should identify the threat from its position in the clock. For example, if someone produces a knife at the nine o'clock position, the executive protection professional should alert the security detail, by sounding off "knife, 9 o'clock." The executive protection professional with the executive should now cover and evacuate the executive towards the 12, 6, or 3 o'clock position, if possible.

Providing protection for an executive does not happen by chance. It is based on a structured and effective approach using *comprehensive protection formations*. Positioning security around and near an executive is not enough and will require the use of strategic protection security formations. The executive protection professional should remain close (arm's reach) to the executive at all times; because the overall objective is to protect the executive from harm and/or embarrassment.

The following formations are used in close-protection security today and have proven to be an effective and resilient tool in the overall security plan. ***Lone formation*** utilizes one security person (executive protection professional) with the executive and can be used in both internal and external movements. The lone formation requires the executive protection professional to stand behind the executive at an angle and not directly behind for better *field of view and observation*.

Secondly, the executive protection professional must maintain an ***arm's reach*** from the executive at all times in the event of an attack. It is important that the executive protection professional remain vigilant and maintain the "arms reach" behind the executive (Dale 2008; Oatman 2006). Some close-protection professionals argue that the executive protection professional should not use their strong arm when executing a cover and evacuate method. Instead, the executive protection professional needs to have the strongest arm ready to retrieve a firearm. In my 30 years of experience, both in the public and private sectors, reaching for a firearm during an attack is a last resort, not to mention that most executives, and corporations in general, have a "no weapon" policy for all staff, including executive security personnel.

A third formation utilized is known as the ***slash or sweep formation***, which requires an *advance person* to lead the protective formation (which is mentioned in the *site advance* section). This formation requires a two-person security team; one as the *advance*, who knows exactly where the team must go, and the *number-one* who is responsible for the safety and security of the executive. Human nature will play a role in how the protective formation is effective when dealing with an attack. Instinct and human reaction many times causes individuals to engage an attacker when their responsibility may have been to the executive. This has occurred and will continue to happen; however, as long as an executive protection professional member within the security detail covers and evacuates the executive, the risk and danger levels are significantly reduced.

A fourth formation is known as the ***wedge formation*****,** which will require three protection security personnel and should be used when a higher threat level has been assessed on the executive. The use of an *advance* person, a *number one* behind the executive and another executive protection professional positioned either to the right or left of the executive can enhance the overall security environment for the executive. This formation is used in public settings where access by the public is possible. Most executives do not use this type of formation for many personal and financial reasons.

Close-Protection Motorcade Security

Motorcade and route management is a primary security mechanism for the executive security plan. Ensuring that the executive and the executive protection professional are safe while being transported will require strategic planning and critical thinking that anticipates danger and other risk concerns. Motorcade sizes may vary, but the fundamentals remain the same (Dale 2008; West 2018). Vehicle transportation is considered vulnerable, because the executive protection professional is not in a *strategic and ready position*. Individuals attempting to kidnap or harm the executive can easily approach and attack the motorcade. Motorcade planning must ensure that the executive protection professional is trained in evasive driving techniques. The executive protection professional driver must operate the vehicle in a safe and responsible manner at all times; and only when under attack should the operator make any evasive moves. The executive should be situated in the right rear of the vehicle to help position the executive for an on-side location arrival.

The executive protection professional must develop *secured routes* when transporting the executive in the motorcade. The first designated route is known as the ***primary route***, followed by a ***secondary route*** and in certain circumstances a ***tertiary route*** may be developed. Multiple routes are needed in the event of an attack, hostile surveillance, or just a traffic condition. The executive protection professional should observe all road and environmental conditions, as well as traffic laws on a particular route. Motorcade route challenges include construction, traffic congestion, demonstrations, roadway chock points, civil unrest, time of day, inclement weather, and pavement condition. The routes should be determined based on safety, but also the ability to evacuate and retreat in the event of an attack. Safe locations or *safe havens* along the route include police stations, fire stations, hospitals, government buildings, and even corporate offices.

The positioning of the motorcade vehicles is critically important and part of a strategic design platform in close-protection security. The theory of aligning cars is part of a security strategy that does not expose the executive unnecessarily and provides tactical positioning for the executive protection professional. After the vehicles have been inspected (checked for improvised explosive devices and mechanical problems), the vehicles are now ready for alignment and positioning. A motorcade configuration should include a *lead car* to pilot the motorcade. The lead car will know the motorcade routes and act as an advance towards identifying hostile surveillance or a dangerous condition that may affect the motorcade's movement (Dale 2008; West 2018). The second vehicle in the alignment usually referred to as the *limo* will transport the executive; and the third vehicle in the motorcade is known as the *follow vehicle;* which will have additional security personnel, if needed.

Known in the field as the *secured package, the* vehicles should be the same make, model, and color so the executive protection professional can rearrange the vehicles when needed to confuse an attacker as to which vehicle the executive may be positioned in. The positioning of the motorcade with the limo in the center also allows the follow-vehicle to become a replacement vehicle for the executive in the event that the limo was to become disabled. Routes for the executive when walking should be with the *flow of traffic* so the motorcade can proceed and continue to shadow the executive at a close distance.

Executive Protection: Residence Security

The executive protection professional will also be responsible for surveying and installing physical security and life safety systems at the executive's residence and/or place of business. Since many attacks, especially kidnapping, have occurred at a person's residence providing productive and effective security protection measures will be a necessary component of the overall executive protection security plan. Implementing physical barriers, such as fencing and motion sensor

lighting will protect the perimeter from a possible intruder. CCTV surveillance cameras should also be installed around the property with remote viewing capability for monitoring the cameras with a smart phone when away from the residence. Exterior protection should also include solid wood doors, ANSI-graded locking devices and anti-fragmentation window filming. Interior rooms of the residence should have intrusion detection sensors on windows and doors, glass break detection, and life safety equipment such as CO2 and smoke detection. Panic buttons must be stationed throughout the residence, i.e., front door area, kitchen, bedroom, gym, and other rooms deemed necessary in the event of attack, injury, or illness. Panic or safe room consideration should also be part of the security survey for rooms within the residence that could be used to shelter the executive.

Executive Protection: International Travel

The executive protection professional will have the responsibility for the security planning and risk analysis when traveling internationally. This can be both complex, as well as frustrating for the EPP because of foreign jurisdictions, culture, language, and international law. Globalization now requires executives to travel aboard to conduct business for the organization. The increased globe footprint requires a robust executive protection plan to increase security and reduce risk for the executive. Whether traveling locally or aboard, the executive protection professionals must apply a comprehensive site advance. However, global travel can be more complex and will require additional planning and logistics.

The executive protection professional should have an interpreter, which the local US Embassy in country can help find. The executive protection professional and the executive must understand the cultural and customs differences before entering the country. Additional concerns include health and medical services for the executive. Having personal experience protecting executives in a developing country, it is a challenge and will test the executive protection professional's ability and knowledge. Protection strategies must consider threats from criminal groups, terrorists, and emotionally disturbed people (West 2018).

Many executives, even in the face of known threats and increased risk, continue to travel abroad. Various locations across the globe are plagued with civil unrest and crime. The risk level will change and the executive protection professional must evaluate all threats and apply security resources as needed. It is critical that the executive protection professional continue to monitor the political climate, as well as any contributing social circumstances within the region. The adoption of a static and inflexible security posture is indicative of poor planning and inexperience.

The USA has available support mechanisms in many regions of the world that can help the executive protection professional when traveling with and protecting an executive. The available resources include the US Department of State and the FBI, who are available to assist and can offer intelligence and threat information on a specific country, region, or specific location. There are also commercial intelligence services that can assist in developing and monitoring current threat and risk levels in a specific country or location. It is recommended that the executive protection professional embrace robust and effective security solutions and do not depend on luck or chance to ensure the safety of the executive.

Prior to the executive's arrival on foreign soil, a security and risk assessment should be made by the executive protection professional in order to calculate the potential for danger. The survey must include all areas that will be visited including official sites, lodging locations, public access locations, and the airport. Part of the assessment should include conferral with the Resident Security Officer (RSO) of the State Department at the US Embassy to inquire about current threat and risk levels within a country or the location you will be visiting (USDS 1997). Commercial third-party security companies are also available to provide security and logistical support for the executive protection professional and the executive when traveling to a foreign destination.

Close-Protection Attire, Appearance, and Equipment

The executive protection professional must wear appropriate attire that is conducive to the professional environment. Like training, professionalism, and attitude, having the proper equipment and presenting a professional look are important in the overall protection of the executive. Protection equipment will vary for the executive protection professional depending on the security environment. The executive protection professional should carry the necessary equipment that will help facilitate the roles and responsibilities. The following equipment is recommended:

- Communications:
  Radio with surveillance kit (earpiece),
  Radio holder (if needed)
  Cellular telephone. Smart phone technology is recommended
- Flashlight:
  Compact flashlight with fresh batteries
- Writing note pad
- Working black ink pen
- Firearm (if authorized) with belt holster and extra magazine clip. Carry permit and other identification for law enforcement purposes.

As a member of the security team, the executive protection professional is on the front lines, not only in regard to an attack, but in the public's eye. Personal appearance is as important as training and both need to be followed and practiced on a continuous basis. The executive protection professional should be groomed and neat. Hair should not be long; it should be combed; finger nails cleaned and have good hygiene.

The required equipment for an executive protection professional is as important as the attire. The executive protection professional should dress in business wear, usually black, dark blue, and grey single-breasted suits. The executive protection professional should also wear a working watch and limited jewelry (Oatman 2006). White shirts and light blue shirts are preferred and ties should match the suit color. Since the executive protection professional can be expected to stand for extended periods of time, *walking* dress shoes of good quality are recommended. Heavy over-coats are not recommended, but a trench coat is the preferred choice. Socks should be dark colored matching the suit or shoes being worn. In certain environments, suits are impractical, like a summer resort. The executive protection professional should have causal clothes in a travel bag at all times. Light weight slacks, like khakis are preferred, along with golf shirts with a collar.

Conclusion

Executive protection is both a challenging and demanding assignment. However, when applied correctly, the executive protection professional will enjoy this assignment for years to come. The ability to meet influential people, global travel, and the many life experiences working as an executive protection professional is worth the effort. The executive protection professional must identify the critical stakeholders when assigned to protecting a senior leader in an organization. The executive protection professional must also realize the differences in cultures within the many different industries, and that corporate cultures vary and are not alike. The executive protection professional should remain humble and learn the fundamentals of executive protection, as each day, a new lesson may be presented.

The executive protection professional should also be careful when working as an "independent contractor" for an organization because of the legal exposure and possibility of a civil suit if actions are taken by the executive protection professional against a person known, or deemed a threat, to the executive. The need for protecting a C-suite executive transcends many levels in a corporation and the executive protection professional must remember that each executive will exhibit a particular personality, level of tolerance, and willingness to follow a security plan. Time will help the executive protection professional better understand the executive's world, the relationship with the executive, and the ability to get the job done.

Cross-References

- ▶ Celebrity Protection
- ▶ Event Security
- ▶ Physical Security: Best Practices
- ▶ Risk Analysis: National and International Standards

References

Blankchtein, B. K. (2013). Executive protection: 4 keys for safe travel. *CSO Magazine, 12*(4), 22.

Dale, J. (2008). *Introduction to executive protection* (2nd ed.). Boca Raton: CRC Press.

Holder, P., & Hawley, D. L. (1998). *The executive protection professional's manual*. Boston: Butterworth-Heinemann.

Kobetz, R. W. (1991). *Providing executive protection*. Berryville: Executive Protection Institute.

N.A. (1997). United States Department of State: Protection Training Manual. USDS.

Oatman, R. (2006). *Executive protection. New solutions for a new era*. Baltimore: Noble House.

West, C. (2018). Corporate executive protection in the 21st century: It's time for a new operating system. *Security: Solutions for Enterprise Security Leaders, 55*(1), 32–33.

Further Reading

Hunsicker, A. (2008). The fine art of executive protection: *Handbook for the executive protection officer.* Boca Raton: Universal Publishers.

West, C., & Jantzen, B. (2016). Corporate executive protection. *An introduction for corporations and security professionals.* Washington: AS Solutions.

F

Federal Emergency Management Agency

Anna Stamper[1] and Lauren R. Shapiro[2]
[1]Homeland Security, Disaster and Emergency Management, Eastern Kentucky University, Richmond, KY, USA
[2]Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Disaster · Emergency management · Emergency operations · Preparedness · Recovery

Definition

The primary purpose of the Federal Emergency Management Agency (FEMA) is to coordinate the response to disasters in the United States that overwhelm local and state authorities while also providing personnel and resources to protect and safeguard life and property, prior to and following disasters.

Introduction

FEMA was founded on April 1, 1979 when President Carter signed *Executive Order 12127* to address the growing need for an agency that primarily focused on helping Americans to deal with disasters. Specifically, FEMA's role is in "preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror" in the United States (see History on FEMA). Since its official inception, FEMA has provided countless resources and conducted disaster relief efforts across the United States, both to prepare for and respond to disasters. FEMA is also the primary agency that oversees the National Flood Insurance Program (NFIP) and is the lead agency in providing aid (both monetary and resources) to communities and citizens affected by disasters. FEMA also handles administrative issues regarding natural disasters and facilitates cooperation between federal agencies, local governments, and affected citizens, when applicable. Table 1 shows the types of FEMA programs and a description of their tasks.

History

The origins of FEMA lie in the Congressional Act of 1803, which was passed to provide assistance

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

Federal Emergency Management Agency, Table 1 FEMA programs and their description of tasks (FEMA 2008)

Program Types	Description of Tasks
Service to Disaster Victims	1. Provides care for victims 2. Assists with multilingual and special need requirements
Integrated Preparedness	1. Works with partners, agencies, and governments to ensure security and preparedness 2. Aids with recovery from attacks, disasters, and emergencies
Operational Planning and Preparedness	1. Works with partner to assist jurisdictions to plan 2. Ensures plans will aid activities
Incident Management	1. Responds to hazards 24/7 2. Trains and certifies staff 3. Works with partners to improve and update standards
Disaster Logistics	1. Implements logistics and procurement systems for 1st responders to plan, identify, track, and distribute supplies 2. Works with partners, donors, and contractors to improve integration and support
Hazard Mitigation	1. Improves risk analysis and hazard mitigation planning to reduce physical and financial impact 2. Implements practices to improve safety and recovery and reduce financial burden
Emergency Communications	1. Works with federal, tribal, state, and local partners to ensure communications 2. Ensures integrated operational link 3. Advocates for disaster emergency communications for 1st responders
Public Disaster Communications	1. Coordinates hazards messaging using public risk, partnership management, and employee communication 2. Provides information for victims, partners, and stakeholders
Continuity Programs	1. Integrates public alert and warning system 2. Provides continuity of government operations and functions

to a New Hampshire town after devastation from a large fire (FEMA 2008). This Act is considered the first piece of legislation passed in the United States addressing disasters and was instrumental in helping legislators recognize the need for disaster legislation. During the following century, ad hoc legislation was passed more than 100 times in response to hurricanes, earthquakes, floods, and other natural disasters (FEMA 2018). Laws unique to each disaster authorized financial assistance to victims and provided both personnel and equipment to assist in recovery and clean up.

In the mid-1930s, as the population increased, more people were being affected by natural disasters. Disaster assistance and recovery became a popular concern among lawmakers and citizens, leading to the Reconstruction Finance Corporation authorizing disaster grants to those affected by disasters (FEMA 2018). Several developments occurred as a result, including the Bureau of Public Roads was able to repair damage to infrastructure (e.g., highways, bridges), the Flood Control Act of 1965 provided projects to build flood control mechanisms, flood insurance was made available for homeowners, and presidents were able to declare disasters (FEMA 2018). However, the financial burden and logistic impact of obtaining help from a variety of agencies during natural disasters led to an increasing need for an efficient and centralized agency to help prepare and recover from disasters so FEMA was created (FEMA 2018).

In 2003, FEMA was integrated into the United States Department of Homeland Security (DHS). (FEMA 2008, 2018; see DHS and DHS Act of 2002 in this encyclopedia). DHS is a cabinet-level department, comprised of 23 separate agencies that allows the government to have a coordinated response to disasters and emergencies affecting national security (see New Mission on FEMA.gov). This restructuring aimed to centralize communication, solve inconsistencies, and secure resources and personnel for FEMA to utilize in major disasters (FEMA 2018; see Emergency Management: Crisis Management and Response; Emergency Management: Emergency Alert

Systems; Emergency Management: Evacuations; Emergency Management: Incident Command System; Emergency Management: National; Human made Disasters; and Natural Hazards in this encyclopedia).

FEMA Costs

Evaluation of FEMA's performance in recent years has resulted in mixed reviews, particularly in light of its costs (DHS 2018). Annual expenditures for FEMA fluctuate depending on the occurrence of disasters (e.g., see DHS 2018). The government was only minimally involved, other than providing US military to help communities following disasters. However, spending has increased in recent decades as a result of both size and frequency increase in federal aid packages as needed by states experiencing often multiple disasters (e.g., California for damage from earthquakes, landslides, and wildfires). According to Edwards (2014): "Annual average FEMA spending was $0.7 billion in the 1980s, $2.8 billion in the 1990s, $13 billion in the 2000s, an $13 billion so far in the 2010s (para 9)." He reported that: "Since 2000, 61 percent of FEMA spending has been for disaster relief, with 20 percent for ongoing preparedness grants to state and local governments, and 12 percent to the National Flood Insurance Program. The remaining 7 percent has been allocated to other programs and administrative costs" (para 10).

Conclusion: The Future of FEMA

While the tasks of FEMA change with every disaster, the new FEMA Strategic Plan is setting the direction for the future and education is an overarching theme of the agency (DHS 2018). In recent years, FEMA officials have implemented two key changes (DHS 2018). First, they have shifted the narrative regarding disaster preparedness, response, and emergency management from a reactive to a proactive approach (see ▶ "Emergency Management: Preparedness and Planning", ▶ "Emergency Management: Recovery", and ▶ "Emergency Management: Incident Command System" in this encyclopedia). Second, they have a heightened focus on educating citizens, first responders, and local officials on disaster preparedness at the community level through the Center for Domestic Preparedness, instead of relying on the government and its agencies to respond following a disaster. FEMA provides online training through its Emergency Management Institute and National Training and Education Division, as well as onsite all hazards training at its Center for Domestic Preparedness (see ▶ "HAZMAT" in this encyclopedia). Congress requires that DHS provide budget overviews for FEMA spending (e.g., DHS 2018). However, there is a need for critical evaluation of federal disaster actions that would allow the government to determine which activities contributed to success and which were inefficient, counterproductive, and a waste of money.

Cross-References

- ▶ Department of Homeland Security (DHS)
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Evacuations
- ▶ Emergency Management: Incident Command System
- ▶ Emergency Management: Preparedness and Planning
- ▶ Emergency Management: Recovery
- ▶ HAZMAT
- ▶ Human-Made Disasters: Electric Power and Transit Linked Outages
- ▶ Human-Made Disasters: Toxic Waste and Residences
- ▶ Natural Hazards

References

Department of Homeland Security. (2018). Federal Emergency Management Agency Budget Overview Fiscal Year 2018 Congressional Justification. https://www.dhs.gov/sites/default/files/publications/FEMA%20FY18%20Budget.pdf. Accessed 6 July 2019.

Edwards, C. (2014). The Federal Emergency Management Agency: Floods, failures, and federalism. https://www.downsizinggovernment.org/dhs/fem3a. Accessed 6 July 2019.

Executive Order 12127, 44 FR 19367, CFR, 1979 Comp., p. 376.

Federal Emergency Management Agency. (2008). Prepared, responsive, committed. FEMA B-653. https://www.fema.gov/pdf/about/brochure.pdf. Accessed 6 July 2019.

Federal Emergency Management Agency. (2018). About the agency. https://www.fema.gov/about-agency. Accessed 6 July 2019.

Further Reading

Fossett, J. W. (2013, July). Let's stop improvising disaster recovery. Nelson A. Rockefeller Institute of Government. https://rockinst.org/blog/lets-stop-improvising-disaster-recovery/. Accessed 6 July 2019.

Government Accountability Office (GAO). (2012, Sept.). Federal disaster assistance: Improved criteria needed to assess a jurisdiction's capability to respond and recover on its own. GAO-12-838. https://www.gao.gov/assets/650/648162.pdf. Accessed 6 July 2019.

Hogue, H. B., & Bea, K. (2006, June 1). Federal Emergency Management and Homeland Security Organization: Historical Developments and Legislative Options. Congressional Research Service report for Congress. https://fas.org/sgp/crs/homesec/RL33369.pdf. Accessed 6 July 2019.

Fire: Evacuation (Engineer Solutions)

Joshua Reichert
Fire Protection and Paramedicine Sciences, Eastern Kentucky University, Richmond, KY, USA

Keywords
Fire protection · Life safety · Egress

Definition

Evacuation, when referring to fire protection and life safety, is the action or notifying and egressing people from a possible hazardous area to a safe location.

Introduction

An efficient evacuation during any emergency event is key to life safety. In order to achieve an efficient evacuation, correct components need to be in place. This includes having a correctly defined evacuation strategy, which is dependent on the scenario, type of building, and occupants involved. This also involves having the correct fire protection devices to detect and notify occupants in a timely manner. Managerial functions must also be taken in to consideration to conduct fire drills and life safety checks to ensure the functionality of the evacuation process.

Evacuation Strategies

To effectively evacuate any building, consideration must be given to the type of building and the occupants in order to determine the best suited evacuation strategy. The most common evacuation strategies include delayed evacuation, phased evacuation, partial or zoned evacuation, total evacuation, and no evacuation (O'Connor and Cohn 2008).

Delayed Evacuation

In cases where a building has occupants with disabilities, there may be a need to provide a safe place for these occupants to evacuate to until they can be assisted to safety. This area is known as an area of refuge and is to be constructed as to protect people from the hazards of fire. NFPA 101 further discusses the requirements of an area of refuge (NFPA 2018). Occupants with disabilities are notified in a similar manner to everyone else that an evacuation is needed, but because they are not able to safely evacuate alone, they evacuate to the area of refuge to await emergency personnel to assist their evacuation.

Phased Evacuation

A phased evacuation strategy, commonly used in high-rise buildings, is used to evacuate those occupying floors closest to the fire first, followed by the rest of the occupants in the building. This

strategy is utilized based on the assumption the fire will not spread too quickly as to affect those waiting for the initial floors to evacuate. This strategy also ensures emergency stairways do not become too densely populated such that the occupants on the fire floor – the ones at the highest risk for exposure to the fire – cannot safely enter the protected stairwell (Tubbs and Meacham 2007).

Partial or Zoned Evacuation

Partial or zoned evacuation relies heavily on passive and active fire protection features. This strategy is best utilized when the evacuation of all occupants requires a tremendous effort and cannot be completed in a timely manner. Hospitals and nursing homes are common places to see a partial or zoned evacuation. For this strategy, only the zone where the fire has been detected is activated, the remainder of the people shelter-in-place (see below). The fire and hazards from the fire are contained in this zone by the use any combination of fire walls, fire barriers, sprinklers, etc. (Tubbs and Meacham 2007, 2008).

Total Evacuation

The most common evacuation strategy is total evacuation. That is, after a fire is detected, everyone is notified, and everyone in the building is evacuated at one time. This is the best strategy in terms of evacuating everyone safely from a building in a timely fashion, but considerations must be given if one of the previously mentioned strategies need to be deployed based on the building and occupant characteristics (Tubbs and Meacham 2007).

No Evacuation (Shelter-in-Place)

In some cases, the best evacuation strategy can be to not evacuate at all. This strategy may also be referred to as protect-in-place, defend-in-place, or shelter-in-place. The idea behind this strategy is to provide an adequate combination of passive and active fire protection features to allow occupants to safely remain in an area. This strategy is common for buildings in which occupants have a difficult time self-relocating. Adequate training of personnel may be required to ensure appropriate actions are taken, such as closing doors to prevent fire and smoke spread (Tubbs and Meacham 2007).

Evacuation Process

During an emergency event, a timely evacuation needs to occur in order to protect lives. When a fire occurs in a structure, the environment is continually being changed by that fire. Temperatures are increasing, visibility is being reduced, toxic chemicals such as carbon monoxide are being released from the fire, structural members are being weakened, etc. At some point, these variables changing the environment will have a limit in which humans can be exposed to before becoming incapacitated and unable to evacuate themselves. These limits that humans can be exposed to before becoming incapacitated are known as tenability limits.

The time between when a fire occurs and when a tenability limit has been reached is known as the Available Safety Evacuation Time (ASET). This would be the amount of time a person has to be notified of a fire event and evacuate before they would become incapacitated and unable to self-evacuate. This time can be determined by an engineering analysis through the use of means such as hand calculations and/or computer fire modeling.

Once the ASET is known, a time scale in which to accurately evacuate people is known. The Required Safety Evacuation Time (RSET) is the amount of time between when a fire occurs and when an occupant reaches a safe location. In order to prevent the loss of lives, the RSET must be lower than the ASET.

RSET is commonly divided into four different variables to calculate. This includes the summation of the time between when a fire ignites and when a fire is detected (time to detection), the time between a fire being detected and the occupants being notified (time to notification), the time between when an occupant is notified and when the occupants begins to egress (premovement time), and the time it takes a person to egress from their starting position to a safe location (movement time).

Time to Detection (t_d)

The time it takes for a fire to be detected will heavily depend on the characteristics of the fire and the detecting method.

Fire Characteristics

Many different variables define the characteristics of a fire and their importance for detecting a fire. The first variable to consider is the growth rate of the fire. Fires are primarily defined by their heat release rate or the rate in which a fire releases energy. As the burning area of a fire grows, the heat release rate typically does too; this is the growth of this fire. Fires with slow growth rates will cause delays in certain types of detection methods.

Coupled with the growth rate of the fire, the soot yield of different types of fuels will influence the detection time. For detectors that activate from an obscuration means require a higher soot yield to reach this obscuration activation threshold, so a fire with a low soot yield will be less effective and cause a longer time to detection for obscuration detectors. Cleaner burning fuels with lower soot yields may require other detection means such as heat detection or air sampling detection.

Detecting Methods

The detecting method will also have a significant impact on how long until a fire is detected. The fastest method of detection will be if the correct detector is selected for the correct scenario. However, it is possible that fire detectors are selected for the wrong possible fire scenario or are not well maintained and do not activate as quickly as they should. The most typical, and quickest, type of detection when properly used and maintained are (NFPA 2019b):

- Ionization smoke detection
- Photoelectric smoke detection
- Combination ionization and photoelectric smoke detection
- Heat detection
- Air sampling detection

Sprinkler systems can also be utilized as a detecting method. Sprinkler systems are required to utilize notification devices, such as water motor gongs or connection to the fire alarm panel to notify occupants. This type of detection will generally be slower than smoke detection devices as sprinkler heads will have activation temperatures that will take longer to reach than the thresholds of smoke detection devices (NFPA 2019a).

Another consideration is scenarios without smoke detectors. In this case, the time to detection relies on the fires to be detected by humans. This involves humans waiting for cues such as visibly seeing smoke, visibly seeing flames, smelling smoke, feeling temperature increases, etc. This is commonly seen in residential homes within smoke detectors, as the fire is allowed to grow unnoticed for a significant amount of time before occupants are made aware of the fire.

Time to Notification (t_n)

Once a fire has been detected by one of the previously mentioned means, the next step is to notify the occupants. The ability to notify occupants will also be heavily reliant on the type of devices present. A fire alarm system required to follow NFPA 72 will require the system to activate all notification devices within 10 s of detection (NFPA 2019b). Notification devices consist of audible notification, visual notification, or other stimuli.

Audible Notification

Two types of audible notification are common; coded notification devices and voice notification devices. A coded notification device sounds in a coded sequence to notify occupants. It is important of anyone that hears a coded fire alarm to quickly interpret it as such, for this reason, in 1996, the American National Standards Institute (ANSI) and the National Fire Protection Association (NFPA) recommended a uniform coded signal known as the temporal-three (T-3) alarm pattern. The T-3 was required for all new construction following this time as required by the 1996 edition of NFPA 72 (NFPA 1996).

Voice notification devices have become increasingly common in fire protection designs.

A voice notification can be a prerecorded message used to inform occupant to evacuate in the case of emergencies. Studies have shown that a voice alarm is more effective than the T-3 alarm due to the fact the voice notification is less ambiguous and hence leads to less misinterpretation when occupants hear the alarm (Nilsson and Johansson 2009; Proulx 1995). Other studies have shown people cannot accurately identify the sound of a T-3 alarm resulting in a low sense of urgency (Proulx and Laroche 2003).

Audible notification selection is important when it comes to waking children. Many studies have shown the T-3 alarm signal is minimally effective at waking children under the age of 10 years (Bruck 1998; Bruck et al. 2004; Thomas and Bruck 2010). In contrast, voice alarms, such as those using the mother's voice, have been demonstrated to be more effective than tone alarms in waking and rousing children to escape (Bruck et al. 2004; Smith et al. 2006, 2018).

Visual Devices

Visual notification devices such as strobe lights are utilized when ambient sound conditions are not conducive for audible notification or if occupants have a hearing impairment. The use of visual notification devices is required by NFPA 72 (NFPA 2019b).

Other Stimuli

There are plenty of other cues that may be available to occupants to notify them of a fire event. These are the same cues previously mentioned in time to detection, in which occupants receive cues directly from the fire itself. In these cases, the time to detection may be long; however, the notification should be short for the person seeing flames or smoke; however, if this person needs to notify others directly, the notification for these occupants may be significant. A similar scenario occurred in the Winecoff Hotel in Atlanta, GA, in 1946. This building did not have a detection and/or notification system, and when the fire was detected, the night manager attempted to phone rooms to warn the occupants of the fire. Hundred and nineteen lives were lost and 90 injured as a result of this hotel fire (McElroy 1947).

Premovement Time (t_p)

After an occupant has been notified and is aware, an evacuation is needed; this occupant has entered the premovement time. The premovement time is any time between when the occupant is notified and when the occupant begins to egress to an exit. The premovement time is the most difficult to predict in evacuation because of the many human behavior factors present. During this time social influences, environmental influences, and cognitive influences may all influence the decision when to evacuate. Document premovement times have been recorded from experiments and real fire event (Fahy and Proulx 2001).

Social Influences

Many social factors can influence people when they are notified of a fire event. The first of which is whether or not the person is alone or not. When a person is surrounded by other people and a fire alarm sounds, occupants are likely to look at each other for cues on whether or not to evacuate (Nilsson and Johansson 2009). This social influence can be linked to people not wanting to be different than the crowd.

Another social factor is whether or not loved ones are present. If an occupant is in a department store and a fire alarm sounds, occupants are likely to seek out those they came to the store with (Shields and Boyce 2000). We see a similar social factor in private residences where mothers will seek out children before they evacuate themselves (Canter et al. 1980).

Environmental Influences

The environment someone is in when notified to evacuate can help determine how quickly the evacuation begins. One comparison that can be made is a person in a public building versus in a house. Homeowners will feel a greater sense of ownership and are more likely to fight the fire to protect the structure than to evacuate it. Renters in a public building are less likely to have of a sense of ownership to the building and will begin to evacuate sooner.

Another environmental factor that influences people before they evacuate can also be seen in the example of homeowners versus renters in the

number of personal belongings. It has been seen that homeowners are more likely than renters to stop to collect their personal belongings before evacuation begins (D'Orazio and Bernardini 2014).

Cognitive Influences

Cognitive factors influence how someone perceives and makes decisions based on previous knowledge and experiences. When a person is notified of a fire event and is aware an evacuation is needed, that person will begin drawing on personal experiences to determine what to do next. People that have experience with fire will have different experiences to draw upon and will act differently than people that do not have those experiences. One cognitive ability people are not well equipped with, which may slow evacuation time, is their ability to predict the growth of fire (Fridolf and Nilsson 2011). In the current social media age, it is not uncommon to see people posting pictures or videos online of a fire instead of evacuating. Part of this reason is due to their inability to accurately predict the fire growth and as a result they delay their evacuation.

Movement Time (t_m)

After an occupant has decided to egress to a safe location and exits to this safe location, this is considered movement time. Movement time takes a few variables in to consideration such as the route an occupant is going to take and the speed in which the person can travel. Once the route is determined (or the distance to the exit), it can be used with the movement speed (distance per time) to determine the movement time.

$$\text{Movement time (minutes)} = \frac{\text{Distance (feet)}}{\text{Speed (feet/minutes)}}$$

Egress Route

When a person begins to evacuate, the same factors as premovement time can influence the route taken. Social influence may influence a person into taking the same route as everyone else, environmental influence may cause someone to be unfamiliar with a building and use the only exit they know (the one they came in), and cognitive influences may allow them to override the other two influences based on their previous experiences and knowledge.

Studies have shown, when people are unfamiliar with a building, most people will utilize the most familiar door, which is usually the primary entrance/exit (Nilsson et al. 2008). This can cause an overcrowding situation along an egress route and increase the overall movement time. Directional signage, along with a voice alarm, has been shown to help prevent this mentality by people evacuating (Galea et al. 2017). Once the route has been selected by the occupant, the overall distance to a safe location can be determined.

Movement Speed

The speed an individual can walk is a function of the density of the area. When a person can walk unimpeded with no one around them on a flat surface, they can walk with full strides, and this average speed is typically around 235 ft./min (1.19 m/s) (Fahy 2008). When a person is moving up and down stairs or through doorways, density will also be a large factor. For this purpose, it is also important to determine the flow (persons/s) and specific flow (persons/min/ft. of effective width) of these locations based on the density. These locations will be slower than previously mentioned and can be considered limiting factors in the movement time calculation. Section 4 Chap. 2 of the *Fire Protection Handbook* provides a full text on calculating egress times (Fahy 2008).

Conclusion

Many factors influence an efficient evacuation. During the initial stages of a building design, consideration should be given to the characteristics of the people that will occupy the building and what characteristics the building itself will have. A full analysis should be conducted using this information to determine the best evacuation strategy to utilize. An engineering analysis can also be conducted through the use of hand calculations and/or computer models to determine if the evacuation strategy and fire protection features utilized

are adequate to provide efficient life safety to the occupants. Engineers can design a building and the egress route as a prescriptive design in which all national and local fire codes are utilized; however, a full engineering analysis to create a performance-based design can be utilized for more unique buildings to show an adequate level of life safety to the occupants achievable through other strategies than what is recommended by code.

Cross-References

- ▶ Fire: Prevention, Protection, and Life Safety
- ▶ Security: Concepts and Definitions

References

Bruck, D. (1998). Arousal from sleep with a smoke detector in children and adults (Report No. FCRC-TR 98-04). London: Fire Code Reform Research Program.

Bruck, D., Reid, S., Kouzma, J., & Ball, M. (2004). The effectiveness of different alarms in waking sleeping children. In *3rd international symposium on human behaviour in fire* (pp. 279–290). https://doi.org/10.1109/LPT.2014.2346396.

Canter, D., Breaux, J., & Sime, J. (1980). Domestic, multiple occupancy, and hospital fires. In *Fires and human behaviour* (pp. 117–136). London: John Wiley & Sons Ltd.

D'Orazio, M., & Bernardini, G. (2014). An experimental study on the correlation between "attachment to belongings" "pre-movement" time. Pedestrian and evacuation Dynamics 2012.

Fahy, R. (2008). Calculation methods for egress prediction. In *Fire protection handbook* (20th ed., pp. 49–68). Quincy: National Fire Protection Association.

Fahy, R., & Proulx, G. (2001). Toward creating a database on delay times to start evacuation and walking speeds for use in evacuation modeling. In *2nd international symposium on human behavior in fire*, Boston (pp. 175–183).

Fridolf, K., & Nilsson, D. (2011). People's subjective estimation of fire growth: An experimental study of young adults. *Fire Safety Science, 10*, 161–172. https://doi.org/10.3801/IAFSS.FSS.10-161.

Galea, E. R., Xie, H., Deere, S., Cooney, D., & Filippidis, L. (2017). Evaluating the effectiveness of an improved active dynamic signage system using full scale evacuation trials. *Fire Safety Journal, 91*, 908.

McElroy, J. (1947). The Hotel Winecoff disaster. *Quarterly of the National Fire Protection Association, 40*(3), 140–159.

NFPA. (1996). *NFPA 72 national fire alarm code*. Quincy: National Fire Protection Association.

NFPA. (2018). *NFPA 101 life safety code*. Quincy: National Fire Protection Association.

NFPA. (2019a). *NFPA 13 – standard for the installation of sprinkler systems*. Quincy: National Fire Protection Association.

NFPA. (2019b). *NFPA 72 – national fire alarm and signaling code*. Quincy: National Fire Protection Association.

Nilsson, D., & Johansson, A. (2009). Social influence during the initial phase of a fire evacuation – Analysis of evacuation experiments in a cinema theatre. *Fire Safety Journal, 44*(1), 71–79. https://doi.org/10.1016/j.firesaf.2008.03.008.

Nilsson, D., Frantzich, H., & Saunders, W. (2008). Influencing exit choice in the event of a fire evacuation. *Fire Safety Science, 9*, 341–352. https://doi.org/10.3801/IAFSS.FSS.9-341.

O'Connor, D., & Cohn, B. (2008). Strategies for occupant evacuation during emergencies. In *Fire protection handbook* (20th ed., pp. 103–111). Quincy: National Fire Protection Association.

Proulx, G. (1995). Evacuation time and movement in apartment buildings. *Fire Safety Journal, 24*(3), 229–246.

Proulx, G., & Laroche, C. (2003). Recollection, identification, and perceived urgency of the temporal-three evacuation signal. *Journal of Fire Protection Engineering, 13*(1), 67–82.

Shields, T. J., & Boyce, K. E. (2000). A study of evacuation from large retail stores. *Fire Safety Journal, 35*, 25–49. https://doi.org/10.1016/j.brat.2014.05.001.

Smith, G. A., Splaingard, M., Hayes, J. R., & Xiang, H. (2006). Comparison of a personalized parent voice smoke alarm with a conventional residential tone smoke alarm for awakening children. *Pediatrics, 118*(4), 1623–1632. https://doi.org/10.1542/peds.2006-0125.

Smith, G. A., Chounthirath, T., & Splaingard, M. (2018). Effectiveness of a voice smoke alarm using the child's name for sleeping children: A randomized trial. *The Journal of Pediatrics, 205*, 1–8. https://doi.org/10.1016/j.jpeds.2018.09.027.

Thomas, I., & Bruck, D. (2010). Awakening of sleeping people: A decade of research. *Fire Technology, 46*(3), 743–761. https://doi.org/10.1007/s10694-008-0065-5.

Tubbs, J., & Meacham, B. (2007). *Egress design solutions: A guide to evacuation and crowd management planning*. Hoboken: Wiley.

Tubbs, J., & Meacham, B. (2008). Selecting appropriate egress strategies. Retrieved from Consulting-Specifying Engineer. https://www.csemag.com/articles/selecting-appropriate-egress-strategies/

Further Reading

National Fire Protection Association. (2008). *Fire protection handbook* (20th ed.). Quincy: National Fire Protection Association.

Society of Fire Protection Engineers. (2016). *SFPE handbook of fire protection engineering* (5th ed.). Gaithersburg: Springer Science+Business Media.
Society of Fire Protection Engineers. (2019). *SFPE guide to human behavior in fire* (2nd ed.). Gaithersburg: Springer Nature Switzerland AG.

Fire: Prescriptive and Performance Based Design

Joshua Reichert
Fire Protection and Paramedicine Sciences,
Eastern Kentucky University,
Richmond, KY, USA

Keywords
Fire protection tactics · Fire protection schemes

Definition

Best practices in the field of fire engineering are procedures that are accepted or prescribed as being correct or most effective.

Strategies for fire engineering is a plan of action designed to achieve an overall aim, usually life safety and property conservation.

Introduction

When architects and engineers collaborate on a new building, extension to an existing building, or renovation to a new building, fire and life safety is always a consideration. A specialty in the fire community that exists to assist with that is fire protection engineers. Fire protection engineering is a professional licensure governed by the state in which the person would like to be licensed in. To become a licensed professional engineer (PE), a person would need to complete a 4-year degree in engineering from an accredited engineering program, pass the Fundamental of Engineering (FE) exam, complete a state-determined number of years working under a licensed PE, and then pass the Principles and Practice of Engineering (PE) exam.

When designing fire protection and life safety for a building, engineers have two best practices in which to choose from: prescriptive design and performance-based design.

Prescriptive design is the design of fire protection features using codes and standards that have been developed for generic buildings. This could include codes and standards from organizations such as the International Code Council (ICC), National Fire Protection Association (NFPA), state and local codes and ordinances, state or local amendments to national codes such as ICC and NFPA, or even corporate codes and standards for fire protection.

The other best practice to design a building with fire protection features is a performance-based design (PBD). Utilizing PBD includes designing the fire protection features specifically for the performance and the functions of the building. To provided a level of safety that is equivalent or exceeds what would be provided using prescriptive design, PBD utilized engineering analysis.

Prescriptive Design

Prescriptive fire protection design is the practice of designing fire protection features per accepted and approved codes and standards. A prescriptive-based code or standard prescribes fire safety for generic use of application. Building codes have a long history in mankind as it has been recognized that responsibility needs to be put on to a building to ensure a level of safety to a building owner. The earliest building code is believed to been written between 1955 B.C. and 1913 B.C. under King Hammurabi of Babylon. Once such building code written stated, “If a house fell and killed the owner of his child, then the building, or his child, would be slain in retaliation” (Foliente 2000).

King Hammurabi identified that buildings should be responsible for the quality of product being handed over to a person that many have no

knowledge of buildings. While mankind has developed and punishments are less extreme, building codes have also developed. Within the United States, different codes and standards exist for use in prescriptive design. While the codes outline a set of rules that knowledgeable people recommend for others to follow. This is not law but can be adopted into law. A standard is the more detailed elaboration of how to meet the code. More specifically, a code tells you what needs to be done and a standard tells you how to do it. These codes and standards help a fire protection engineer develop a prescriptive strategy for designing fire protection.

The ICC was established in 1994 as a nonprofit organization dedicated to developing a single set of comprehensive and coordinated national model construction codes. The formation of the ICC was due to three separate nonprofit organizations which were developing separate sets of model codes to be used in the United States. The three separate organizations were the Building Officials and Code Administrator International, Inc. (BOCA), International Conference of Building Officials (ICBO), and Southern Building Code Congress International, Inc. (SBCCI). It was recognized one single organization was needed without regional limitation; hence the formation of the ICC was made a realization (ICC).

Currently, the ICC produced 15 different codes covering different concentrations. Pertaining to fire protection design, the most important codes published by the ICC are the International Building Code (IBC), the International Fire Code (IFC), the International Plumbing Code (IPC), and the International Residential Code (IRC) (ICC n.d.).

International Building Code – This code is the foundation for all codes from the ICC. It has been accepted by most jurisdictions within the United States as well as some jurisdictions internationally.

International Fire Code – This code is designed to meet the needs to address conditions hazardous to life and property from fire, explosion, handling or use of hazardous materials and the use and occupancy of buildings and premises. This code establishes minimum regulations for fire prevention and fire protection systems using both prescriptive and performance-related provisions.

International Plumbing Code – This code sets minimum regulations for plumbing systems and components to protect life, health, and safety of buildings' occupants and the public. The IPC covers a range of topics such as backflow prevention, fixtures and fittings, water supply and distribution, etc. These covered topics are important when designing sprinkler systems for a building.

International Residential Code – This code is designed to address one- and two-family dwellings and townhouses of not more than three stories above grade. The IRC covers aspects of construction such as building, plumbing, mechanical, fuel gas, and electrical, which all play a role in fire prevention and fire protection of residential structures.

The National Fire Protection Association (NFPA) is also another organization that creates and publishes prescriptive codes, standards, and recommended practices. NFPA was formed in 1896 and has been devoted to eliminate death, injury, and property and economic loss due to fire and electrical and related hazards. NFPA, as of 2018, delivers information and knowledge through more than 300 consensus codes and standards, research, training, education, outreach, and advocacy. Each code and standard through NFPA are revised and updated every 3–5 years and normally take about 2 years to complete (NFPA n.d.).

Jurisdictions, both state and local, regulating building design and fire protection must adopt codes in order to become law. Jurisdictions may also determine the codes are not strict enough in certain areas and opt to either not adopt the national codes, but to write their own to enforce. Jurisdictions may also decide to adopt the national codes but to write amendments to certain parts of the code. For example, the state of Georgia adopts ICC codes such as the IBC and IFC but have amendments to certain sections of the codes (Georgia Department of Community Affairs n.d.).

Performance-Based Design

Performance-based design (PBD) is the second practice that an engineer may use to design fire protection features for a building or process. The Society of Fire Protection Engineers (SFPE) has developed a strategy for performing a performance-based design for fire protection titled, *SFPE Engineering Guide to Performance-Based Fire Protection* (SFPE 2007).

SFPE was established in 1950 and incorporated as an independent organization in 1971. As of 2018, the society has over 4600 members and 92 chapters, including 17 student chapters worldwide. It is the mission of SFPE to "define, develop, and advance the use of engineering best practices; expanding the scientific and technical knowledge base; and educate the global fire safety community, to reduce fire risk" (SFPE n.d.).

In the guide, SFPE has developed a step-by-step guide to conducting a performance-based design.

Step 1: Define Project Scope

Defining the scope of a project should always be the first step in any design project. Without a well-defined scope, it is possible to not fully understand how to accomplish this project and cause errors that could cost money at later stages in the design process. Some of the information needed when defining the scope includes the constraints on the design and the project schedule, building construction and features desired, occupant characteristics, building characteristics, and applicable codes and regulations.

Step 2: Identify Goals

Once the objectives of the project are understood, it is easier to define the goals of the project. This should always include the levels of protection for people and property. Other considerations for a goal could be preservation of historical buildings or items, business continuity, and protection of the environment.

Step 3: Define Objectives

The objectives of the design project are the design goals with tangible values for evaluation purposes. This could include dollar value loss, loss of life, or any other impacts from a fire event.

Step 4: Develop Performance Criteria

This step includes developing the performance criteria that the design will be expected to meet. This is a further refinement of the design objectives and will include items such as tenability limits for life safety. The tenability limits will need to be well-defined and agree upon between all authorities and engineers to continue forward with the project.

Step 5: Develop Design Fire Scenarios

This step could include extensive research and a good understanding of the function of the building in which the fire protection features are being design for. By taking the building type and function into consideration, fire scenarios can be derived. This could include expected fuel packages, locations, peak heat release rates, growth rates, and products of combustion. An adequate amount of fire scenarios should be selected to ensure all possible worst-case scenarios have been tested again the fire protection design.

Step 6: Develop Trial Designs

This step is where the actual fire protection features are introduced. Consideration should be given to what the stakeholders and building owners would like within the building. This could include proposed fire protection systems, construction features, and operations. At this step in the design process, an engineering and all approving parties should determine and agree how the evaluation of each fire scenario to each trial design is going to occur. Typical evaluation techniques include hand calculation and computer fire modeling.

Fire protection hand calculations are widely known and used within the fire protection community. While hand calculations are quick and time-efficient, most are empirical correlations and have limitations. Hand calculations are also good for small-scale applications and become too difficult and tedious for large-scale buildings for a performance-based design.

Computer fire modeling has become revenant in the fire protection community for performance-based design. Computer fire models are usually divided into two categories, two-zone models and field models.

Two-zone models divide a computational domain into two zones, typically upper and lower layer within a compartment. Two-zone models have a low computational demand and can be more efficient on small scales but still have limitations. An example of a two-zone model is the Consolidated Model of Fire and Smoke Transport (CFAST), which is a free computer fire model maintained by the National Institute of Standards and Technology (NIST) (NIST n.d.-a).

Field models, also known as computational fluid dynamic (CFD) models, divide the computation into a user-specified number of zones. This allows for adjustments to the number of calculation zones; however, with an increased number of zones comes an increase in computational demand. Many field models exist in industry; one such is named Fire Dynamics Simulator (FDS) and is a free computer fire model maintained by the NIST (NIST n.d.-b).

Step 7: Evaluate Trial Designs

The next step in the design project is testing the chosen fire scenarios against the trial fire protection designs utilizing the chosen evaluation technique. The evaluation technique should provide analytical data that can be used to compare to the performance criteria.

Step 8: Determine if Design Meets Performance Criteria

Any trial fire protection designs that fail to meet the performance criteria for any of the fire scenarios can either be altered to change or increase fire protection features, or other means of fire protection must be considered. If any of the trial fire designs pass the performance criteria for all of the fire scenarios, this design can be deemed adequate to meet all the objectives of the project. However, it is likely none of the trial fire protection designs pass the performance criteria for fire scenarios, and this could be caused by restricting objectives, goals, or performance objectives, too severe of fire scenarios, or even incorrect use of the evaluation method. If no trial fire protection designs pass the performance criteria for all the fire scenarios, these possible restrictions may need to be readdressed, and the process starts over.

Step 9: Select the Final Design and Report

If there are more than one trial fire protection designs that pass the performance criteria for all fire scenarios, then one trial design will need to be selected. With more than one option, this allows the building owner to determine which design best fits their monetary and design needs. All steps of this performance-based design should be documented in a final report. This final report should be approved by additional engineers, authority having jurisdiction (AHJ), and all stakeholders.

Conclusion

Fire protection design is a field in which is very dynamic. New fire hazards and new building designs are always going to keep this field from remaining static. Fire protection professionals have a few best practices and strategies to achieve adequate fire protection to provide life safety for occupants. The use of national and local building and fire codes provide a generic best practice and strategies to design the fire protection features. If buildings do not fit the mold of the generic codes, it may be more beneficial, or needed, for a fire protection professional to conduct a performance-based design. In order to do so, the fire protection industry has stabled some best practice and strategies in a step-by-step guide to insure success when conducting this type of design. Either strategy should ensure the objectives of the codes and standards are met to ensure things such as life safety, building protection, and environmental protection.

Cross-References

► Fire: Prevention, Protection, and Life Safety
► Security: Concepts and Definitions

References

Foliente, G. (2000). Developments in performance-based building codes and standards. *Forest Products Journal, 50*, 12–21.

Georgia Department of Community Affairs. (n.d.). *Georigia State Amendments to the International Building Code (2012 Edition).* Retrieved from https://dca.ga.gov/sites/default/files/2014_ibcamendments.pdf

ICC. (n.d.). *About ICC*. Retrieved from International Code Council: https://www.iccsafe.org/about-icc/overview/about-international-code-council/

NFPA. (n.d.). *About NFPA*. Retrieved from National Fire Protection Association: https://www.nfpa.org/About-NFPA

NIST. (n.d.-a). *CFAST, fire growth and smoke transport modeling.* Retrieved from National Institute of Standards and Technology: https://www.nist.gov/el/fire-research-division-73300/product-services/consolidated-fire-and-smoke-transport-model-cfast

NIST. (n.d.-b). *FDS and smokeview.* Retrieved from National Institute of Standards and Technology: https://www.nist.gov/services-resources/software/fds-and-smokeview

SFPE. (2007). *SFPE engineering guide to performance-based fire protection*. Bethesda: Society of Fire Protection Engineers and the National Fire Protection Association, Inc.

SFPE. (n.d.). *About SFPE*. Retrieved from Society of Fire Protection Engineers: https://www.sfpe.org/page/About?

Further Reading

Society of Fire Protection Engineers. (2007). SFPE engineering guide to performance-based fire protection. National Fire Protection Association, Quincy, MA.

Hurley, M., & Rosenbaum, E. (2015). *Performance-based fire safety design*. Boca Raton: CRC Press.

Society of Fire Protection Engineers. (2015). *SFPE handbook of fire protection engineering*. New York: Springer.

Fire: Prevention, Protection, and Life Safety

Joshua Reichert
Fire Protection and Paramedicine Sciences,
Eastern Kentucky University,
Richmond, KY, USA

Keywords
Fire mitigation

Definition

Fire protection is the methods and actions to reduce and mitigate the effects and damage caused by a fire event.

Fire prevention is the methods and actions taken to reduce the likelihood of a fire event.

Life safety is the primary goal in fire protection utilizing a method or system to protect the life of occupants.

Introduction

The United States and mankind in general have always had a fire problem. What was and has always been one of the most important tools to the human race can quickly become one of the deadliest. Humans learned to harness fire for many uses such as to cook food and stay warm. But just as fire has good applications, it has its bad sides as it burns down buildings and cities, destroys forests, and takes lives when out of control.

Fire protection has been seen as early as 300 B.C. by the Romans as a slave fire department. By A.D. 26 a full-time fire department in Rome was flourishing and was charged with enforcing fire prevention safeguards and punishing any person that did not follow the safeguards or was responsible for a fire event (Robertson 2005).

Many attempts to mitigate the impact of fires have also been seen throughout time. The Great London Fire of 1666 destroyed approximately 13,200 houses, 87 churches, and 50 livery halls over an area of 436 acres (Cote 2004). The primary construction material in London at the time was wood and straw. However, this fire enforced a need to prevent the spread of fire from one building to another, which lead to the way London looks today, with majority of construction being brick and stone.

Today, fire protection is the application of fire prevention and fire mitigation to provide life safety, property conservation, and environmental protection. The fire protection field consists of, but is not limited to, fire fighters, fire

marshals, fire prevention officers, fire protection engineers, fire protection specialists, fire investigators, etc. The best ways to achieve adequate fire protection are to provide fire prevention and, if a fire does occur, mitigate the impact of the fire as much as possible. Many best practices and strategies are incorporated into providing adequate fire prevention and fire mitigation.

Fire Prevention

Fire prevention has many levels associated with it. Prevention starts before products are even released to distributors or retailers by testing regulated by government agencies. However, not all fire events can be prevented, and for that reason, fire education is provided as a secondary fire prevention method.

Consumer Product Fire Prevention

In recognition of the fact that manufacturers and distributors should not be allowed to release products to a consumer without consideration to the safety of the product, laws such as the Consumer Product Safety Act (CPSA), Flammable Fabrics Act (FFA), etc. were enacted to give regulatory power to the Consumer Product Safety Commission (CPSC).

The CPSC is an independent federal regulatory agency formed in 1972. It is the mission of the CPSC to protect the public against unreasonable risks of injury or death from consumer products through education, safety standards activities regulations, and enforcement. The CPSC is committed to protecting consumers and families from products that pose a fire, electrical, chemical, or mechanical hazard (United States Consumer Product Safety Commission n.d.).

In order to educate the public and consumers of potential harm or ensure consumers of safety products, the CPSC releases technical reports. These reports are not always written and published by the CPSC as they may release technical reports conducted by other entities within the government, such as the National Institute of Standards and Technology (NIST). Further education is provided by the CPSC in the form of Residential Fire Loss Estimates. This provides the public such as consumers, manufacturers, distributors, and even fire departments with the ability to identify fire trends and allow the public to adjust accordingly.

The CPSC enforces consumer product safety under given laws/acts regulating different products or substances utilizing federal regulations. These regulations are named the Code of Federal Regulations (CFR). The CFR is published by the Federal Register by the executive department and agencies of the federal government of the United States. The CFR is divided into 50 titles covering a broad range of subjects. Both fire prevention and fire protection areas can be found located in different Titles of the CFR.

Fire Prevention Programs

Despite federal regulations, fires still occur in all types of locations with potential for harm. The next line of defense to prevent these fires are fire prevention programs. One of the most recognizable and longest lasting fire prevention program is that of Smokey Bear.

In 1944, the US Forest Service and the Ad Council agreed that a fictional bear would be the symbol for their joint effort to promote forest fire prevention. By 1947, and to this day, Smokey Bear's slogan, "Only YOU Can Prevent Forest Fires!" is still widely known (Office of Communication 2014).

Other national organizations also provide fire prevention programs. Every year in October, the nation recognizes Fire Prevention Week and is considered the longest running public health observance. Fire Prevention Week was first enacted in 1925 by President Calvin Coolidge in commemoration of the Great Chicago Fire of 1871. The National Fire Protection Association (NFPA) has been the official sponsor of Fire Prevention Week since its enactment. Every year, NFPA promotes a different fire prevention theme to the public (NFPA n.d.).

Local fire departments, paid, volunteer, and combination, are all known to provide fire prevention programs to their community. Many fire departments around the country have a Fire Prevention Officer charged with such programs. It is

possible for fire departments to use both local and national statistics to determine trouble areas to focus on for fire prevention or for fire departments to focus on the highest risk demographic of their community. It is common for fire departments to offer fire prevention demonstrations for the community and programs for younger children. Fire departments also have authority to conduct facility inspections to ensure code compliance, which is also a form of fire prevention.

Employers are also in charge of providing a workplace safe from recognizable fire hazards. The Occupational Safety & Health Administration (OSHA) was created in 1970 when President Richard Nixon signed the Occupational Safety & Health Act of 1970 (Occupational Safety & Health Administration n.d.). OSHA regulates employers through standards and enforces violations of said standards. OSHA requires employers to provide fire prevention measures such as, but not limited to, safeguards to fire hazards, training to workers on potential fire hazards, and fire safety plans.

Fire Protection

Fire protection is a large industry around the world with many different parties involved. Two methods are used to provide adequate fire protection. The first method is fire prevention, if a fire never occurs, then adequate fire protection has been achieved. Fire prevention can be provided by eliminating a hazard of a product or process, educating all involved parties on the fire hazard, or providing administrative or engineering controls to the fire hazard. If fire prevention is unsuccessful, the second method to adequate fire protection is needed, and that is to mitigate the impact of the fire event. Mitigating the effects of the fire can be done by limiting how large the fire can grow and by containing the fire to one location until the fire can be suppression.

Active Fire Protection

Active fire protection is the first line of fire protection in the event of a fire and typically comes in two forms: fire detection and fire suppression.

If a fire is to occur, it is essential to notify occupants as soon as possible to ensure adequate life safety. To do so, automatic fire detection is installed. Detector devices can be spot type detectors that only notify the local area or can be linked to a panel to notify a facility in the case of detection. Many types of automatic fire detection devices are available for use and include, but are not limited to ionization smoke detectors, photoelectric smoke detectors, combination smoke detectors, heat detectors, beam detectors, and air sampling detection.

Ionization smoke detectors – these smoke detectors contain a small amount of radioactive material between two electrically charged plates. If smoke is present, it disrupts the current of ions between the two plates and activating the alarm. This type of smoke detector is generally more responsive to flaming fires.

Photoelectric smoke detectors – these smoke detectors utilize a light source that is aimed into a sensing chamber at an angle away from the sensor. When smoke enters the sensing chamber, it reflects the light source into the sensor activating the alarm. This type of smoke detector is generally more responsible to smoldering fires.

Combination ionization/photoelectric detectors – this is a combination of functionality between ionization smoke detectors and photoelectric smoke detectors to cover a spectrum of fire scenarios. This allows a smoke detector to have the sensitivity of each time of smoke detector for both flaming and smoldering combustion.

Heat detectors – two types of heat detectors are common for use: rate-of-rise detectors and fixed temperature detectors. A rate-of-rise detector activates if the temperature increases too quickly over a specified period of time. A fixed temperature detector activates if a specified temperature is reached. These detectors have good application in facilities where ionization and photoelectric detectors may be prone to false alarms such as facilities that accumulate dust.

Beam detectors – these types of detector devices are good for use in large spaces such as atriums and warehouses. To use, a transmitter is located at one end of the coverage area and is pointed at the receiver at the other end of the coverage area. If anything happens to disrupt the transmitted beam, the detector activates.

Air sampling – air sampling smoke detector is a series of pipes (usually CPVC) with small holes at intervals of the pipe. The pipe directs back to an air sampling unit which pull air from the pipes to sample what is returned to the unit for smoke. If smoke is identified by the air sampling unit, activation occurs.

Fire suppression is also another common type of active fire protection. Suppression can provide two functions in a fire event, fire detection (if other detection means are not present or malfunctions) and suppression/containment of the fire event. Many types of fire suppression agents are in use today including, but not limited to, water, water mist, FM200, foam, wet chemical, dry chemical, NOVAC 1230, and carbon dioxide.

Passive Fire Protection

In fire protection, it is also important to contain the fire to one location and protect the structure to prevent structural damage; this is achieved through passive fire protection. Many structures and products can be used to achieve adequate passive fire protection. When the purpose is to compartmentalize a fire and prevent it from spreading to other parts of a building, this can be achieved with components such as fire walls, fire barriers, fire partitions, fire doors, and fire curtains and shutters.

Fire walls, barriers, and partitions – fire walls are structures built from the base of a building to the roof. Fire wall ratings can range from 3 h to 4 h. Fire barriers differ from fire walls as they only extend from floor to floor or floor to roof including any concealed spaces. Fire barrier ratings can range from 2 h to 3 h. Fire partitions in all respects are similar to fire barriers but have a fire resistance rating of 1 h to 2 h. Fire walls, barriers, and partitions must be constructed of materials that have been tested and rated in accordance with ASTM D 119, ISO 834-1, EN 1363-1, or AS/NZ 1530 (XL Catlin n.d.).

Fire doors – fire door assemblies must be tested in accordance with NFPA 252, UL 10B, BS 476: Part 20, or EN 1634-1. Fire doors must be installed and maintained in accordance with NFPA 80 and GAP.2.2.2 (XL Catlin n.d.).

Fire curtains and shutters – fire curtains and shutters are based on the same principle, a type of fire or smoke separator that can be stored in a hidden place that will deploy in the event of a fire and activation of the fire protection system. Fire curtains are usually made of a more flexible material, while fire shutters are made of a more rigid material, leading to fire shutters having a higher fire and smoke resistance rating. Each fire or smoke resistance rating will be dependent on the testing to have been performed on a product by an approved laboratory.

Manual Suppression

The final line of defense in fire protection is using humans to manually suppress a fire. It is likely manual suppression by an occupant of a building could occur before a fire suppression system activates but is not likely. It is more expected to see manual suppression in structures with no automatic suppression.

Fire extinguishers are one available tool to be utilized in manual suppression activities. Fire extinguishers range in sizes anywhere from 5lbs of chemical to extinguishers on carts to be moved to a fire for manual suppression. The extinguishing agents within fire extinguishers also vary depending on the recognized fire hazards in that location. Fire extinguishers follow a hazard classification system to determine the type of extinguisher to use for a given fire event.

Class A: Class A fuels are ordinary combustibles such as wood, paper, cardboard, cloth, etc.
Class B: Class B fuels are flammable liquids and gases such as gasoline, propane, etc.
Class C: Class C fuels are live electrical equipment such as printers, computers, etc.

Class D: Class D fuels are combustible metals such as magnesium, lithium, etc.
Class K: Class K fuels are cooking oils and fats common to a kitchen setting.

Fire extinguishers will be labeled with these different classifications to signify their appropriateness for a type of fire. Depending on the extinguishing agent in the fire extinguisher will determine the classification of fire it is available to extinguish. Some extinguishing agents will be capable of extinguishing more than one classification of fire and will be labeled as so (e.g., ABC fire extinguisher).

If a fire grows to a point where manual suppression by occupants or workers is no longer a safe option, the next manual suppression option is by trained fire personnel (fire departments or fire brigades). Firefighters engage to two types of manual suppression activities, interior and exterior fire attacks. For an interior fire attack, firefighters wear personal protective equipment (PPE) and enter the structure with a fire attack hose line. Firefighters will move throughout the structure to find the fire and extinguish the fire with water and in some cases foam. If the trained fire personnel determine a structure is no longer safe for an interior fire attack, they will deploy larger hose lines and begin an exterior attack in an attempt to extinguish and contain the fire from further spread to other buildings.

Life Safety

Fire prevention and fire protection are all focused around providing adequate life safety to residents, workers, visitors, customers, etc. Life safety is the primary goal of all aspects of fire protection from the fire prevention professional, to the firefighter, to the investigators. Life safety has been such an important goal to the fire protection field that NFPA has named an entire code after the fact, NFPA 101 *Life Safety Code*. This code is one of the most widely adopted and used code, not just within the United States, but also around the world. This code covers both fire prevention and fire protection features and activities.

Conclusion

The fire protection field is a large industry with many different concentrations and focuses. The hazards presented to the fire protection field are always changing and evolving as mankind moves to the future with new technologies. The fire protection field will always need to adapt and research new methods and technologies to address the endless changing hazards presented. This will always be done with the focus of life safety as the primary goal. The fire community will always firstly attempt to prevent any fire. This is usually the cheapest and easiest fire management strategy to ensure life safety. If prevention of a fire event is unachievable, then the fire community has many fire protection methods and activities available to protect human life.

Cross-References

► Security: Concepts and Definitions

References

Cote, A. (2004). *Fundamentals of fire protection*. Quincy: National Fire Protection Association.
NFPA. (n.d.). *About fire prevention week*. Retrieved from National Fire Protection Association: https://www.nfpa.org/Public-Education/Campaigns/Fire-Prevention-Week/About-Fire-Prevention-Week
Occupational Safety & Health Administration. (n.d.). *OSHA at 30: Three decades of progress in occupantional safety and health*. Retrieved from United States Department of Labor: https://www.osha.gov/as/opa/osha-at-30.html
Office of Communication. (2014, August 4). *The story of Smokey Bear*. Retrieved from U.S. Forest Service: https://www.fs.fed.us/blogs/story-smokey-bear
Robertson, J. (2005). *Introduction to fire prevention* (6th ed.). Upper Saddle River: Pearson Education.
United States Consumer Product Safety Commission. (n.d.). Retrieved from https://www.cpsc.gov
XL Catlin. (n.d.). *Fire walls, fire barriers and fire partitions*. Retrieved from XL Catlin: https://xlcatlin.com/-/media/gaps/221____0.pdf.

Further Reading

Cote, A. E. *Fundamentals of fire protection*. Quincy: National Fire Protection Association.

Robertson, J. C., & Love M. T. *Robertson's introduction to fire prevention*. Upper Saddle Ridge: Pearson Education.
Klinoff, R. *Introduction to fire protection*. Clifton Park: Delmar Learning.
Gagnon, R. M. *Design of special hazard and fire alarm systems*. Clifton Park: Delmar Learning.
NFPA 101. *Life safety code*. Quincy: National Fire Protection Association.
NFPA 221. *Standard for high challenge fire walls, fire walls, and fire barrier walls*. Quincy: National Fire Protection Association.

First Responders: Police

Heather A. Panter
Centre for Advanced Policing Studies, Liverpool John Moores University, Liverpool, UK

Keywords
Emergency services · Firefighters · Police · EMT · Accident response · Decision-making

Definition

Typically, first responders (i.e., individuals who render aid at an emergency scene) include police officers, firefighters, rescuers, paramedics, emergency medical technicians (EMT), and any other individual responsible for emergency responses. Effective responses to emergency calls can play a critical role in the treatment of a victim, treatment of an arrestee, securing the scene, preserving the scene, and successful transfer of authority and responsibility of the scene to secondary responders.

Introduction

Initial actions undertaken by first responders set the stage for how emergencies and critical incidents are effectively managed. The main basic goals of responding first responders are to gain control of a site/situation and to manage available resources successfully (see Alison et al. 2015; Power and Alison 2017; Trenholm 2018). Further, there exist competing responsibilities of the first responder to render aid, avoid becoming a casualty, secure the scene, preserve and document the scene, and release the scene to appropriate authorities. As such, this entry focuses on the actions that the first responder – police officer – on a scene should carry out while managing competing responsibilities.

From a police perspective, anything and everything could be an emergency that requires first responder interactions. Further, police power itself is arguably essential to the construction of social order, and it is always an emergency power (Correia and Wall 2018). Therefore, police are referred to as "first line of defense" or "first responders" because of the perpetual management in emergency responses. Further, "policing" is the everyday application of emergency prerogatives while using discretion to make decisions on effective responses (Correia and Wall 2018). Police discretion involves individual judgements made by officers of which several behavioral responses maybe appropriate in specific situations. Outside of policing, discretion to other first responders (e.g., firefighters, EMTs) similarly entails how work policies, laws, operating procedures, and perspectives of safety interact with decisions on how to react, the extent of reaction, and on what occasions. Within policing, first responder discretion further entails what laws to enforce, the extent in which they should be enforced, against whom, and on what occasions (Schulenberg 2015).

Securing the Scene

The first priority of any first responder is personal safety and ensuring that the scene is made safe. Before a first responder's arrival to a scene, dispatch advises responders of any safety considerations that 911 callers have identified, but often these safety considerations are incomplete or contradictory. This creates uncertainty and leads to four questions:

1. Is there a criminal still at scene who can assault non-police personnel and police personal alike?;
2. Will relatives of a victim turn violent towards emergency workers?;

3. What kind of hazards will be present?;
4. Are there man-made or natural hazards present that can inhibit or harm first responders? (Gardner 2011).

Often police are called the "blue canaries" of first responders for several reasons. First, police vehicles are often quicker to emergency scenes due to their size and ability to negotiate heavy traffic areas and therefore they are frequently first upon scenes. Secondly, police approach fires or accidents involving potentially hazardous materials without any breathing apparatus or protective gear (Gardner 2011). Etymologically, "blue canaries" refers to the use of canaries in coalmines to detect hazardous gases. Thus, firefighters are often credited with a more conscious approach to hazards as they approach an emergency situation. Comparatively, police handle calls often "in progress" with due care and caution with a less emphasis upon risk management in static scenes (see Gardner 2011).

In non-static scenes (scenes with danger still being present), first responders must take control of the scene and focus on lifesaving activities. If human suspects are a safety concern, police officers are responsible for controlling and limiting actions of suspects, and at times, victim/witnesses. Suspects on scenes represent a higher level of concern and a higher priority due to officer-safety issues (Gardner 2011). Notably, before any lifesaving and fire rescue responses can take place, police officers must sweep scenes for suspects and render the scene safe. For example, in a shooting situation with multiple causalities, police first responders must ensure that the direct threat (the shooter) is apprehended or away from the scene before firefighters and EMTs can treat/transport victims. Further, police first responders have to ensure that victims are not suspect(s) themselves while making efforts to preserve the scene.

Preserving the Scene

For safety and forensic reasons, first responders are tasked with defining the criteria for incident boundaries. The criteria for doing so include focal points, avenues of entry and exit, and secondary scenes (Gardner 2011). Notably, initial boundaries established by first responders may change based upon reassessment by secondary responders. Because first responders establish these boundaries in non-stable environments, unlike secondary responders when the environment is more stable, reassessment by secondary responders of incident size, incident location, and further safety variables is common. For example, during a response to a homicide, the initial crime scene is often roped off farther than that initially assessed by responding homicide investigators.

Notably, regardless of the type of emergency, scene integrity should be upheld. From a police perspective, this is equated to crime scene evidence from being destroyed and contaminated (Gardner 2011). From all emergency perspectives, this is also equated to ensuring that the continuing safety of those within incident boundaries do not face additional hazards and reduce the ones that are currently present (i.e., structural hazards, chemical/bioterror hazards, mass causality situations, etc.). This process entails managing who has access to said incident boundaries and what secondary access points are viable (Gardner 2011). Additionally, an incident personnel log should be maintained to account for any possible forensic (e.g., trace evidence transfer) and safety considerations (Gardner 2011). As such, at all times, it is imperative that movement of first responders is accounted for regardless of the emergency they are facing.

First responders are also critical in determining the secondary response composition. Secondary responders, as indicated by first responders, define tactically the nature and scope of secondary response. For example, during a vehicle entrapment with hazardous chemicals, first response firefighters may request specialist fire units and EMT units to assist as secondary responders. Notably, the more complex an incident scene appears, the more likely an integrated specialist secondary response team might be required according to the assessment of first responders. When police respond to a bombing incident where structural hazards may be present, the expertise of

firefighters may be used as a primary line of defense for police and crime scene technicians (Gardner 2011). In more extreme situations, the expertise of structural engineers might be relied upon to keep the scene safe.

In mass casualty situations, a multijurisdictional response is often required. Concerns in a multijurisdictional response involve initial oversight into how to communicate and operate as a cohesive team and how resources can become quickly depleted (Gardner 2011). This became a major highlighted issue during 9/11 when police, EMT, and fire jurisdictions were unable to talk via radio to one another. While most emergency agencies have pre-event planning coordination responses, often the first responder is tasked with initially accessing risk management in multiagency responses (see Alison et al. 2015; Hu et al. 2014; Power and Alison 2017). Therefore, first responders must identify hazards, assess hazard(s) risks, control and reduce the effect of a hazard, and supervise how the hazard is initially managed with multiple emergency responders prior to releasing a scene to secondary responders (see Alison et al. 2015; Power and Alison 2017).

Releasing the Scene to Secondary Responders

Eventually, after ensuring proper documentation, first responders will have to release the scene to secondary responders (e.g., criminal investigators, EMTs, and fire fighters who must await for the scene to be secured; hazmat technicians; technical rescue technicians; utility workers; emergency volunteers; civil engineers; etc.). During this downtime, while awaiting secondary responders, first responders may begin taking notes for the documentation process. During this process, initial observations, actions upon initial arrival, and specific details about the incident assist in the relaying of vital information to secondary responders for a debriefing. Therefore, effective documentation about what the first responder knows, what they found, and what they did should be relayed to secondary responders when handing the scene over (Gardner 2011).

Conclusion

First responder actions set the stage for success and safety of secondary responders. Therefore, first responders are tasked with initial scene assessment and how sources should be allocated. During this process, first responders must ensure that they do not become a casualty, document all information, provide and coordinate emergency care, secure the incident scene and those found there, and subsequently release the scene to determined secondary responders.

F

Cross-References

- ▶ Arrest
- ▶ Critical Infrastructure: Emergency Services Sector
- ▶ Emergency Management: Crisis Management and Response

References

Alison, L., Power, N., van den Heuvel, C., Humann, M., Palasinksi, M., & Crego, J. (2015). Decision inertia: Deciding between least worst outcomes in emergency responses to disasters. *Journal of Occupational and Organizational Psychology, 88*(2), 295–321.

Correia, D., & Wall, T. (2018). *Police: A field guide*. London: Verso Books.

Gardner, R. M. (2011). *Practical crime scene processing and investigation*. Boca Raton: CRC Press.

Hu, Q., Knox, C. C., & Kapucu, N. (2014). What have we learned since September 11, 2001? A network study of the Boston marathon bombings response. *Public Administration Review, 74*(6), 698–712.

Power, N., & Alison, L. (2017). Offence or defence? Approach and avoid goals in the multi-agency emergency response to a simulated terrorism attack. *Journal of Occupational and Organizational Psychology, 90*(1), 51–76.

Schulenberg, J. L. (2015). Moving beyond arrest and reconceptualizing police discretion: An investigation into the factors affecting conversation, assistance, and criminal charges. *Police Quarterly, 18*(3), 244–271.

Trenholm, S. B. (2018). *Identifying the necessary components of a police decision-making model*. Doctoral dissertation, Memorial University of Newfoundland.

Further Reading

Baudour, C., & Bergeron, J. (2016). *Emergency medical responder: First on scene* (10th ed.). Boston: Pearson.

LeMay, J. (2016). *CSI for the first responder: A concise guide*. Boca Raton: CRC Press.
Madigan, M. L. (2017). *HAZMAT guide for first responders*. Boca Raton: CRC Press.

Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats

Pierre-Luc Pomerleau[1] and Mathieu Auger-Perreault[2]
[1]Business Administration – Homeland Security and Leadership Policy, Northcentral University, San Diego, CA, USA
[2]Cybersecurity, Georgia Institute of Technology, Atlanta, GA, USA

Keywords
Analytics · Artificial intelligence · Authentication · Cloud computing · Cybercrime · Fraud · Insider threat · Machine learning · Payments

Definition

Fraud is the loss of financial assets, information, or property where a victim unknowingly believes false information provided by a malicious individual or organization that stands to benefit from the false representation.

Introduction

Organizations of all sizes recognize that fraud, whether committed by malicious insiders or external threat actors, can have a significant impact on an organization's reputation and profitability as well as on customer experience. Firozabadi et al. (1998) claim fraud usually occurs when: "(a) an individual or an organization intentionally makes an untrue representation about an important fact or event; (b) the untrue representation is believed by the victim (the person or organization to whom the representation has been made; (c) the victim relies upon and acts upon the untrue representation; (d) the victim suffers loss of money and/or property as a result of relying upon and acting upon the untrue representation" (Firozabadi et al. 1998, p. 4). Fraud has been researched for decades, giving birth to fraud models that seek to understand the various factors involved in fraudulent activities, including pressure to commit fraud, the opportunity that allows the fraud to occur, and the rationalization the fraudster uses to justify his behavior.

Large corporations, such as WorldCom and Enron, have declared bankruptcy as a result of the malicious actions of insiders (Binns 2019), while others, such as the French bank Société Générale, have suffered billions in losses (Hunker and Probst 2011). With the increased popularity of e-commerce and the migration to electronic banking and payments, the external threat has become digital (Abu-Shanab and Matalqa 2015), providing fraudsters with new opportunities. Billions of records, including personal identifiable information, have been stolen as part of massive data breaches (Cheng et al. 2017). For example, in 2013, hackers stole information about 40 million Target credit cards and 70 million personal information records, while Yahoo reported that all 3 billion of its user accounts had been compromised (McMillan and Knutson 2017). More recently, the personal information of 148 million Americans was exposed in the Equifax data breach (Fleishman 2018).

Fraudsters either sell such stolen information and the tools used to extract it in illicit marketplaces (Dupont et al. 2017) or leverage the data for illegal purposes, such as using social engineering and spear-phishing attacks to trick targets into providing confidential information, perform fraudulent transactions, or make it possible to install malware on victims' computers (Butavicius et al. 2016). Spear-phishing differs from traditional phishing – which involves sending email to a massive number of individuals but expecting only a small response – in that attackers have personal information about their victims and can target specific individuals within an organization. Their emails include relevant information

about their victims, increasing the likelihood that victims (often chief executive officers, executives, or accounting and finance personnel) will click on a link and/or provide confidential information.

Data analytics has been used to prevent and detect fraud for decades, using methods that range from detection rules to artificial neural networks. Detection rules are based on expert knowledge and can be easily explained to client organizations, the management, or potential users. However, to keep up with the ever-changing tactics of fraudsters, rules must continually be added to or adjusted to remain relevant, and monitoring their effectiveness is complicated. They must also be maintained in an inventory, and their performance tracked, leading to complex and time-consuming rules management systems. While a single rule is easily explainable, having hundreds of rules nullifies that advantage (Ryman-Tubb et al. 2018).

Machine learning models have also been used to prevent and detect fraud, most notably in credit card fraud management. There are three categories of machine learning models: supervised, unsupervised, and reinforcement, with supervised and unsupervised learning the most prevalent in fraud risk management. Supervised learning algorithms, such as decision trees, logistic regression, and support vector machines, require labeled data, such as confirmed fraudulent transactions. Unsupervised learning, such as clustering, does not use labeled data and is useful in fraud risk management as it facilitates detection of anomalies. A confusion matrix can be used to assess the performance of a machine learning detection model (Ryman-Tubb et al. 2018).

Data visualization, by highlighting outliers or duplicate payments in potential fraudulent transactions, has also been used in fraud detection and investigation. Another data visualization technique that shows anomalies in a dataset is Benford's Law, which states that the distribution of numbers in many data sets, including those in nature, follows the same pattern, with "1" as their first digit 30.1% of the time, "2" 17.6% of the time, "3" 12.5% of the time, and so on. Comparing the distribution of numbers in a dataset to distribution according to Benford's Law can highlight outliers that may be indicative of fraud (Durtschi and Pacini 2004). Regardless of the analytic technique used, its performance must be tracked, and false positive and fraud detection rates are often used to assess performance (Ryman-Tubb et al. 2018). In fraud detection, a true positive (TP) is a confirmed fraud incident detected by the model. False negatives (FN) are instances of confirmed fraud that the model did not identify. False positive (FP) refers to non-fraud events that the model incorrectly identified as fraud, and true negative (TN) refers to non-fraud events that the model correctly identified as non-fraud. The fraud detection rate of a model can therefore be calculated as TP / (TP + FN), while the false positive rate can be calculated as FP / (TN + FP) (Sokolova and Lapalme 2009).

Artificial intelligence (AI), defined by Chandra and Prihastomo (2012) as creating a system by which a machine can perform tasks like a human, has also been used in fraud detection. Machine learning, a way of trying to achieve AI, is the ability of computer systems to learn and improve through experience rather than explicit instructions. Several machine learning algorithms have been developed, such as decision trees, support vector machines, and neural networks. While decision trees are easily explainable, other machine learning algorithms, despite active research, remain black boxes, which stifle their adoption rate, especially in heavily regulated industries.

Research in AI has taken place since the 1950s, with cycles of hype and "AI winters" (Menzies 2003, p. 18). Deep learning, a machine learning technique at the heart of many recent advancements in computer vision and speech recognition, is based on neural networks, which have been studied for decades. One key difference between the use of AI today and AI in the 1990s is the amount of data and computing power available. According to Schmidhuber (2007), the Internet and, more recently, the Internet of Things (IoT) are contributing factors in the vast amount of data available today. Cloud computing allows computing to be pooled, on demand, enabling machine learning techniques to be used on extensive datasets. Fraud risk management, anti-money

laundering, and cybersecurity risk management practices, combined with on-demand computing resources, benefit from the increased amount of available data.

Cloud Computing and the Rebirth of AI

The term artificial intelligence is not new. It was first used in 1956 during the Dartmouth Conference (Gryz 2013), and sparked research into how computers could be made to think like humans. In 1958, artificial perceptron was invented, increasing hopes for advancements in AI. For example, in 1965, Herbert A. Simon, a renowned economist and AI pioneer, was quoted as saying that "machines will be capable, within twenty years, of doing any work that a man can do" (Gryz 2013). However, this hopeful period was followed by a significant reduction in AI funding, called an AI winter, and then another cycle of hope and winter. Several breakthroughs in the 1990s put AI back into the mainstream. For example, in 1997, Deep Blue, a chess-playing AI program developed by IBM, defeated world champion Garry Kasparov (Campbell 1999). The 1990s also saw the rise of the World Wide Web, an invention at the heart of a level of generation of data never seen before in history, most notably through the Internet of Things (Zaslavsky et al. 2013). This large amount of data improved the possibilities for AI, as machine learning algorithms require a great deal of data to make better predictions (Gandhi et al. 2017). According to Vaquero et al.:

> Clouds are a large pool of easily available and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), also allowing for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which the Infrastructure provider offers guarantees using customized SLAs [service-level agreements]. (Vaquero et al. 2009, p. 2)

Machine learning has proven its effectiveness in many fields, and machine learning interpretability is an active area of research. However, in a heavily regulated industry, such as banking, opacity is still an obstacle to mass adoption and trust. Tulio et al. (2016, p. 1) propose two definitions of trust in a machine learning context: "(1) trusting a prediction, i.e., whether a user trusts an individual prediction sufficiently to take some action based on it, and (2) trusting a model, i.e., whether the user trusts a model to behave in reasonable ways if deployed." The authors note the importance of interpretability in getting users to adopt and trust a model and its predictions, for example, by making clear which variables or features are essential to the prediction. Prediction explanations are also useful in choosing between two models that both perform well in terms of other metrics, such as accuracy (Tulio et al. 2016).

External Fraud

External fraud can take various forms. Financial institutions have dealt with some of them for decades, with cheque fraud, identity theft, and counterfeit credit cards responsible for significant losses (Smith 2018). In the 1990s, fraud involving credit card transactions led banks to adopt fraud detection systems that evaluate the risk associated with each transaction. These systems usually combine rule management with alert management (Ryman-Tubb et al. 2018). Fraud investigators are then tasked with confirming if the transactions associated with an alert are legitimate or not. This feedback is then used to adjust models and detection rules.

Recognizing that counterfeit fraud led to significant losses, financial institutions, in partnership with various card providers, decided to invest in Europay Mastercard Visa (EMV) cards or what is referred today as chip cards. Chip cards, unlike magnetic stripe cards, use dynamic data elements to reduce the risk of counterfeiting (Anderson and Murdoch 2014). With counterfeiting opportunities for credit cards reduced by EMV, fraudsters migrated online, initiating fraudulent e-commerce transactions as well as data breaches. Some of these data breaches targeted credit card information (Smith 2018). Armed with data from credit cards, fraudsters try to either initiate fraudulent transactions or sell the

information in illicit marketplaces. However, buyers and sellers on such marketplaces know that it is only a matter of time before banks detect the fraud and cancel the cards and malicious actors have therefore begun to steal personal information, which, unlike credit card information, is not open to being changed or replaced (Dupont et al. 2017). Significant data breaches at Yahoo and Equifax resulted in billions of records becoming available in illicit marketplaces (Smith 2018), making it possible for criminals to try to open new accounts or to obtain loans and other services under stolen identities. As mentioned earlier, the information is also used to send targeted phishing emails.

Fraudsters have also migrated to wire-transfer fraud. One type of wire-transfer fraud is Business Email Compromise (BEC), in which criminals use social engineering to trick people into transferring funds to another country. Messages that appear to be from an authority figure, the CEO for example, are sent to an employee, asking that funds be moved quickly by wire transfer to an overseas country where the CEO is supposedly on a business trip. Many organizations have fallen for this crime, to the point that the Federal Bureau of Investigations (FBI) estimates that losses related to BEC amount to billions (Federal Bureau of Investigation 2018). Criminals have also targeted several banks around the world, asking them to send fraudulent wire transfers through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) platform. In the last few years, there have been several cases of banks getting hacked, most notably the Bank of Bangladesh and Punjab National Bank. In the case of the Bank of Bangladesh, criminals infiltrated the bank's system and initiated close to a billion dollars in wire transfers – US$81 million was eventually lost after it was sent to bank accounts in the Philippines opened by criminals using fictitious identities (Karim 2016). In the case of Punjab National Bank, two employees used the SWIFT system to issue fraudulent letters of undertaking worth over US$1 billion (Gayathri and Mangai 2018). These cases highlight the need to take a holistic approach to fraud risk management, as both outsiders and insiders can take part in fraudulent activities. It is worth noting that the Bank of Bangladesh case, as well as other cybersecurity events such as the hack into the Bank Muscat (Musaev and Yousoof 2015), show the convergence of cybersecurity and fraud. A cybersecurity event such as a hacking incident can lead to fraud transactions. Such situations have led some organizations to create centralized fusion centers, where professionals from both fraud and cybersecurity departments share information about threats and prevention mechanisms and establish standard incident-response procedures.

Organizations have realized they need to improve their fraud mitigation measures. One key piece of the fraud management puzzle is authentication. While identification is concerned with who you are (e.g., username, email address), authentication focuses on proving that you are who you say you are. While the most popular authentication mechanism is still the password (Choubey and Choubey 2013), there are several issues with password-based authentication. First, many users have weak passwords that are easily guessable or that can be found in leaked password databases available on the Internet or the dark web. Also, users tend to have the same password for different platforms, so a malicious actor who gets access to a database of email addresses and associated passwords can try to reuse these combinations on other websites. This is what happened in the 2012 LinkedIn hack, in which millions of email addresses and passwords used to log into LinkedIn were stolen by cybercriminals (Walters 2016).

To strengthen authentication measures, organizations are moving away from a single authentication factor (something you know) to multifactor authentication: something you know (e.g., password), something you are (e.g., biometrics), or something you have (e.g., a trusted device). Biometrics can be broken into several categories, with various degrees of security and intrusiveness (Jain Ross and Prabhakar, 2004) and its use in authentication has become more mainstream in recent years, most notably through Apple's use of fingerprinting technology to unlock a phone or to pay with it. Device profiling is another component of enhanced authentication. By analyzing a

device, an organization can leverage hundreds of data points (e.g., browser type, operating system, screen resolution) and assign a risk level to a device. Based on this risk level, an enhanced authentication method can be used, for example, through SMS (short message service) or a push notification to an application on a trusted device. Authentication is one piece of the fraud mitigation puzzle; analytics is another.

Insider Threat

Insider threat is part of a new reality for public and private organizations. An insider threat is an individual (e.g., a contractor) or an employee working inside the organization who has legitimate access to critical assets and privileges based on a position of trust within the organization (Catrantzos 2012). Understanding the motivations behind fraud has been the subject of many studies, with the fraud triangle – the theory that fraud is most likely to occur when individuals encounter pressure, opportunity, and find a way to rationalize the resulting actions that do not conflict with their values – and the fraud diamond – the fraud triangle plus capability; when the fraudster do realize he has an opportunity as well as the "ability to turn it into reality" – two of the most popular approaches (Abdullahi and Mansor 2015). Numerous factors can lead an employee or an individual working inside the organization to decide to attack it. The most common are: (a) personal predisposition, (b) personal stressors, and (c) professional stressors (Ozkaya and Aslaner 2019). Insiders may attempt to profit directly from fraud or may intend to damage the company by stealing data or destroying information and critical assets or to damage its reputation by revealing sensitive, proprietary, or confidential information. The reasons for such actions are not always rational and may be related to frustrations such as a promotion they did not receive, a salary increase that did not live up to their expectations, or loss of a job.

Insider threats may also be motivated by less personal reasons, such as being paid by a competitor to sabotage activities or having built relationships with organized crime (Pomerleau 2019). Criminals may enlist employees to help commit crimes such as drug trafficking, launching a cyberattack, or physical attacks against the organization or an individual (Shapiro et al. 2018; Ozkaya and Aslaner 2019; Pomerleau 2019). Malicious employees know the level and responsibilities of employees within the organization and may leak information that assists outsiders to target another employee with a convincing email that includes proprietary data to make it look like a legitimate request (Ozkaya and Aslaner 2019). Malicious employees may also benefit from selling personal information about clients to organized crime organizations, which use this information to apply for credit cards and loans.

An insider threat may also occur when an employee fears being penalized by his employer for an innocent mistake. For instance, an employee might be a victim of a phishing fraud scam that makes it possible for the hacker to encrypt all the information on the employee's work computer. The attacker may then ask the employee to pay a ransom to get his data back, and if the employee is too embarrassed to discuss the matter with his supervisor or to report the incident to the internal security department, he or she may pay the ransom, leading to additional ransom demands (Gordon 2018). Even if the employee regains access to the data, the software, malware, or Trojan horse used by the hacker may still be in the organization's system, making it possible for the attacker to access other critical information or systems (Gordon 2018). If such a security incident takes place, and the organization is not aware of it in time to take remedial actions, it may lead to more critical business interruptions, losing access to crucial information, or problems with significant business dealings that will significantly impact the organization's bottom line as well as its reputation (Gordon 2018).

Ozkaya and Aslaner (2019) used Accenture survey data about cyberattacks on various organizations to estimate the extent of financial losses related to cybercrime and found that insider threat is now the most common type of cybercrime and leads to the highest average losses. In 2017, the average loss per incident was US$173,516, and

the authors suggest that it usually takes 50 days to recover from such an attack. Indirect costs, production loss, and the cost of business downtime also need to be taken into consideration in managing insider threat cases (Lobo 2019). When responding to such an attack, a forensic investigation may be necessary, various legal procedures may be needed to recover the stolen information, and a root cause analysis is recommended best practice. Such a postmortem analysis makes it possible to understand why the incident occurred and what additional preventive and investigative controls should be implemented to avoid a similar situation in the future. Insider threats incidents may also lead to the creation of a crisis cell within the organization, as the malicious employee may have stolen customers' personal information. If this is the case, the organization will need to communicate with affected customers and take appropriate mitigating measures to protect the identity and privacy of their clients.

To protect themselves, organizations need to have the proper tools in place. These tools might be intrusion prevention and detection systems, data loss prevention systems, or security incident management (SIEM) systems to monitor logs and detect suspicious activities in employees' behavior. Fraud detection capabilities, rules, and models that are currently used to identify external fraud can be leveraged to detect insider threat. For example, security professionals need to understand what regular actions or behaviors are and what should be considered suspicious. For instance, is it normal for an employee working a regular day shift schedule to try to get access to a confidential file at night from an unknown IP address while connected through the virtual private network (VPN)? Is it normal for an employee leaving the organization to download many files onto a USB key on his last day at work? If an employee is sending multiple emails with large documents attached from his corporate email to a personal email account, it should trigger an alert for review to see what actions should be taken. When analyzing a suspicious occurrence, an investigation analyst might ask if an employee with high-privilege access has shared his login access with a hacker, making it easier for an outsider to get access to confidential data and systems (Ozkaya and Aslaner 2019).

Various strategies and techniques can be used to prevent and detect insider threat before an unfortunate incident occurs. Unfortunately, this type of threat management is far from being a perfect science as such threats are incredibly challenging to prevent. Organizations can use data analytics, machine learning, and intelligence sharing within their organization as well as with external partners (Pomerleau 2019). Vetting personnel through background checks before hiring, job rotations within the organization, and making sure to apply least privileges and separation of duties rules are still the foundational prevention measures that every organization should implement (Ozkaya and Aslaner 2019). Different tools and data analysis techniques, such as those mentioned earlier, can also help identify abnormal behavior. While small organizations may not have security teams dedicated to managing insider threats, these organizations should still try to have minimal prevention and detection capabilities in place to detect suspicious transactions or anomalies in behavior that do not fit with regular employee activities. Within large organizations, fraud investigation, corporate security, and cybersecurity teams should share as much intelligence as possible as this is one of the most efficient and effective ways of managing insider threat cases. A dedicated team should be responsible for data analytics, rules, and models as this puts it in a better position to identify potential insider threat behavior and makes it possible to act before it is too late to protect the organization.

Conclusion

In this entry, we look at the evolution of fraud risk from the perspective of both external fraud and insider threat. We also discuss how data analytics has been used in fraud risk management, as well as the key indicators that should be utilized to evaluate performance. We look at how AI has evolved since its beginnings and how the amount of data and computing power has changed in the past 15 years. While there is no silver bullet in

fraud risk management, recent advances in AI are promising. These advances will, however, also be used by those seeking to commit fraud. The cat and mouse game played by fraud professionals and criminals will continue, meaning that organizations need to invest in data analytics techniques such as machine learning and AI to mitigate risks for their organizations as well as to protect their customers.

Cross-References

- Big Data
- Insider Threat
- Investigations: Bank Fraud
- Investigations: Employee Theft of Employer Property
- Investigations: Fraud
- Machine Learning
- Public-Private Partnerships: Port Security

References

Abdullahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. Retrieved from https://pdfs.semanticscholar.org/d86f/5988fccc216c92c891191323a2c7f639b834.pdf

Abu-Shanab, E., & Matalqa, S. (2015). Security and fraud issues of E-banking. *International Journal of Computer Networks and Applications, 2*(4), 179–187. Retrieved from https://www.ijcna.org/Manuscripts/Volume-2/Issue-4/Vol-2-issue-4-M-04.pdf

Anderson, R., & Murdoch, J. S. (2014). EMV: Why payment systems fail. Retrieved from https://cacm.acm.org/magazines/2014/6/175170-emv/abstract

Binns, C. A. (2019). Investigations: Fraud. In L. Shapiro & M.-H. Maras (Eds.), *Encyclopedia of security and emergency management*. Cham: Springer.

Butavicius, A. M., Parson, K., Pattinson, R. M., & McCormac, A. (2016). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. Retrieved from https://www.semanticscholar.org/paper/Breaching-the-Human-Firewall%3A-Social-engineering-in-Butavicius-Parsons/b58de02e690f07853e88cc93e93e5b71fdf9b493

Campbell, M. (1999). Knowledge discovery in Deep Blue. Retrieved from https://dl.acm.org/citation.cfm?id=319396

Catrantzos, N. (2012). *Managing the insider threat: No dark corner*. Retrieved from https://www.amazon.com/Managing-Insider-Threat-Dark-Corners/dp/1439872929

Chandra, R., & Prihastomo, Y. (2012). Artificial intelligence definition: A review. Retrieved from https://www.semanticscholar.org/paper/Artificial-Intelligence-Definition-%3A-A-Review-Chandra-Prihastomo/d959ad041acca7570a7229e51c18a297bb7ca0b2

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *WIREs: Data Mining & Knowledge Discovery, 7*(5). https://doi.org/10.1002/widm.1211.

Choubey, J., & Choubey, B. (2013). Secure user authentication in internet banking: A qualitative survey. Retrieved from https://www.researchgate.net/publication/290465488_Secure_User_Authentication_in_Internet_Banking_A_Qualitative_Survey

Dupont, B., Côté, M. A., Boutin, I. J., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world". *American Behavioral Scientist, 61*(11), 1219–1243. https://doi.org/10.1177/0002764217734263.

Durtschi, C., & Pacini, C. (2004). The effective use of Benford's Law to assist in detecting fraud in accounting data. Retrieved from https://www.researchgate.net/profile/Cindy_Durtschi/publication/241401706_The_Effective_Use_of_Benford's_Law_to_Assist_in_Detecting_Fraud_in_Accounting_Data/links/54982f4a0cf2c5a7e342a59e.pdf

Federal Bureau of Investigation. (2018). International business e-mail compromise takedown: Multiple countries involved in coordinated law enforcement effort. Retrieved from https://www.fbi.gov/news/stories/international-bec-takedown-061118

Firozabadi, S. B., Tan, H. Y., & Lee, M. R. (1998). Formal definitions of fraud. Retrieved from https://pdfs.semanticscholar.org/f10b/ff42c86d957ce6aa0c3fd69f23f77eacfb5e.pdf

Fleishman, G. (2018). Equifax data breach, one year later: Obvious errors and no real changes, new report says. Retrieved from http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

Gandhi, D., Pinto, L., & Gupta, A. (2017). Learning to fly by crashing. Retrieved from https://arxiv.org/pdf/1704.05588.pdf

Gayathri, S., & Mangai, T. (2018). A critical analysis of the Punjab National Bank scam and its implications. *International Journal of Pure and Applied Mathematics, 119*(12), 14853–14866. Retrieved from https://ssrn.com/abstract=3274568

Gordon, W. R. (2018). Information sharing and collaboration. In A. K. Sood (Ed.), *Canadian cybersecurity 2018; An anthology of CIO/CISO enterprise-level perspectives* (pp. 107–128). Retrieved from https://issuu.com/clxforum/docs/canadian-cybersecurity_2018

Gryz, J. (2013). The frame problem in artificial intelligence and philosophy. Retrieved from https://www.cambridge.org/ca/academic/subjects/philosophy/

philosophy-mind-and-language/cambridge-handbook-artificial-intelligence?format=HB&isbn=9780521871426

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats an overview of definitions and mitigation techniques. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.7490&rep=rep1&type=pdf

Jain, K. A., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. Retrieved from https://people.eecs.berkeley.edu/~johnw/cs294-97/papers/intro-biometric.pdf

Karim, S. S. (2016). Cyber-crime scenario in banking sector of Bangladesh: An overview. Retrieved from http://www.icmab.org.bd/images/stories/journal/2016/Mar-Apr/3.Cyber-crime.pdf

Lobo, S. (2019). Understanding the cost of a cybersecurity attack: The losses organizations face. Retrieved from https://hub.packtpub.com/understanding-the-cost-of-a-cybersecurity-attack-the-losses-organizations-face/

McMillan, R., & Knutson, R. (2017). Yahoo triples estimate of breached accounts to 3 billion. Retrieved from https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804

Menzies, T. (2003). Guest editor's introduction; 21st-century AI: Proud, not smug. Retrieved from https://www.computer.org/csdl/magazine/ex/2003/03/x3018/13rRUxC0SLS

Musaev, E., & Yousoof, M. (2015). A review on internet banking security and privacy issues in Oman. Retrieved from http://icit.zuj.edu.jo/ICIT15/DOI/E-Technology/0070.pdf

Ozkaya, E., & Aslaner, M. (2019). *Hands-on cybersecurity for finance: Identify vulnerabilities and secure your financial services from security breaches*. Retrieved from https://www.amazon.com/Hands-Cyber-Security-Finance-vulnerabilities-ebook/dp/B07F2JH 2YF/ref=sr_1_1?keywords=cybersecurity+for+finance&qid=1554684802&s=books&sr=1-1

Pomerleau, P. L. (2019). Public-private partnerships: Port security. In L. Shapiro & M.-H. Maras (Eds.), *Encyclopedia of security and emergency management*. Cham: Springer.

Ryman-Tubb, F. N., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence, 76*, 130–157. https://doi.org/10.1016/j.engappai.2018.07.008.

Schmidhuber, J. (2007). 2006: Celebrating 75 years of AI – History and outlook: The next 25 years. Retrieved from https://arxiv.org/abs/0708.4311

Shapiro, L. R., Maras, M.-H., Velotti, L., Pickman, S., Wei, H.-L., & Till, R. (2018). Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security, 11*(3/4), 65. https://doi.org/10.1007/s12198-018-0191-3.

Smith, S. (2018). Investigations: Bank fraud. In L. Shapiro & M.-H. Maras (Eds.), *Encyclopedia of security and emergency management*. Cham: Springer.

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing & Management, 45*(4), 427–437. Retrieved from http://atour.iro.umontreal.ca/rali/sites/default/files/publis/SokolovaLapalme-JIPM09.pdf

Tulio, R. M., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. Retrieved from https://www.kdd.org/kdd2016/papers/files/rfp0573-ribeiroA.pdf

Vaquero, L., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. *Computer Communication Review, 39*(1), 50–55. Retrieved from http://ccr.sigcomm.org/online/files/p50-v39n1l-vaqueroA.pdf

Walters, R. (2016). Cyber attacks on U.S. companies in 2016. Retrieved from http://thf-reports.s3.amazonaws.com/2016/IB4636.pdf

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013) Sensing as a service and big data. Retrieved from https://arxiv.org/abs/1301.0159

Further Reading

Isson, J. P. (2018). *Unstructured data analytics: How to improve customer acquisition, customer retention, and fraud detection and prevention*. Retrieved from https://www.amazon.ca/Unstructured-Data-Analytics-Acquisition-Prevention/dp/1119129753/ref=tmm_hrd_swatch_0?_encoding=UTF8&qid=&sr=.

Mitchell, M. T. (2017). *Machine learning*. Retrieved from https://www.amazon.com/Machine-Learning-Tom-M-Mitchell/dp/1259096955/ref=sr_1_2?keywords=machine+learning+mitchell&qid=1555379101&s=books&sr=1-2

Ozkaya, E., & Aslaner, M. (2019). *Hands-on cybersecurity for finance: Identify vulnerabilities and secure your financial services from security breaches*. Retrieved from https://www.amazon.com/Hands-Cyber-Security-Finance-vulnerabilities-ebook/dp/B07F2JH2YF/ref=sr_1_1?keywords=cybersecurity+for+finance&qid=1554684802&s=books&sr=1-1

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Retrieved from https://www.amazon.com/Security-Risk-Management-Information-Paperback/dp/B015QL5S22/ref=sr_1_fkmrnull_3?keywords=Security+risk+management%3B+Building+an+information+security+risk+management+program+from+the+ground+up&qid=1555378999&s=books&sr=1-3-fkmrnull

G

Geographic Information Systems (GIS) Applications in Emergency Management

Hung-Lung Wei
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, CUNY, New York, NY, USA

Keywords
GIS · Emergency management · Natural hazards · Technological hazards

Definition

Burroughs (1986) defined GIS as "a powerful set of tools for collecting, storing, retrieving, transforming, and displaying spatial data from the real world" (quoted in Waugh 2002, p. 277). In addition, Star and Estes (1990) stated GIS as "An information system that is designed to work with data referenced by spatial or geographic coordinates. In other words, a GIS is both a database system with specific capabilities for spatially referenced data, as well as a set of operations for working with the data" (p. 2).

Introduction

Geographic Information Systems (GIS) is a computer-based information system that can be utilized to acquire, store, display, and analyze spatial data; and it is widely used in the field of emergency management. Drabek (1991) defined emergency management as "the discipline and profession of applying science, technology, planning and management to deal with extreme events that can injure or kill large numbers of people, do extensive damage to property, and disrupt community life" (p. xvii). Thus, emergency managers should apply best methods to mitigate for, prepare for, respond to, and recover from the risks of catastrophic events. The importance of GIS has been recognized by many local, state, and federal government officials, private sectors, and hazard scholars who have applied a variety of GIS tools to deal with issues of emergency management. Specifically, this entry describes some examples of GIS application for natural and technological hazards.

Natural Hazards

In the past decades, natural hazards (e.g., hurricanes, tornadoes, tsunamis, earthquakes, volcanic eruptions, floods, landslides, wildfires, etc.) have caused a number of casualties and economic losses

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

worldwide. Federal Emergency Management Agency (FEMA) developed a GIS-based software – Hazus – to estimate potential losses from earthquakes, floods, and hurricanes (see https://www.fema.gov/hazus). This GIS-based software can be utilized for four phases of emergency management – mitigation, preparedness, response, and recovery – and it is widely adopted and used by emergency management organizations in the United States, Singapore, Canada, Australia, and Pakistan (Islam and Ryan 2015). Moreover, in 2003, FEMA initiated a Flood Map Modernization (Map Mod) program, as part of the National Flood Insurance Program (NFIP) to update the flood maps and to provide accurate flood risk data in GIS format on the Digital Flood Insurance Rate Maps (DFIRMs). Through this program, 95% of the paper flood maps were eliminated and transformed into a GIS-based digital inventory of flood hazard data (Islam and Ryan 2015). The US National Oceanic and Atmospheric Administration (NOAA) developed the Sea, Lake and Overland Surges from Hurricanes (SLOSH) model to estimate storm surge heights resulting from historical, hypothetical, or predicted hurricanes by taking into account the atmospheric pressure, size, forward speed, and track data (see https://www.nhc.noaa.gov/surge/slosh.php). Based on this SLOSH model, in 2016 NOAA created the Potential Storm Surge Flooding Map program to predict risk areas associated with coastal flooding from storm surge (see https://www.nhc.noaa.gov/surge/inundation/). Regarding the earthquake hazard, the US Geological Survey (USGS) developed an Earthquake Hazards Program that provides earthquake data including real-time and historic earthquake catalogs, GIS data, and seismic hazard analysis tools that create customized hazard maps to assess individual and overall hazard (Islam and Ryan 2015).

In addition to government efforts, a substantial number of hazard scholars have utilized GIS tools to determine the proximity of natural hazard sources, and they found that people's perceived risk is associated with the proximity of natural hazard sources – volcano (Blong 1984; Gregg et al. 2004; Johnston et al. 1999; Wei and Lindell 2017), earthquake (Palm et al. 1990), and hurricane (Baker 1991; Lindell et al. 2005; Lindell and Hwang 2008; Peacock et al. 2005; Zhang et al. 2010).

Technological Hazards

Like natural hazards, technological hazards (e.g., toxic chemicals, radiological and nuclear materials, flammable materials, and explosives) can cause injuries, fatalities, and property damages. In the United States, hazardous materials (hazmat) are regulated by many federal agencies such as Department of Transportation (DOT), Environmental Protection Agency (EPA), Nuclear Regulatory Commission (NRC), etc.; however, FEMA and US Coast Guard are responsible for emergency responses to hazmat incidents. The hazmat is categorized as "explosives, gases, flammable liquids, flammable solids, oxidizers and organic peroxides, toxic (poisonous) materials and infectious substances, radioactive materials, corrosive materials, and miscellaneous dangerous goods" (Lindell et al. 2006, p. 139). Emergency managers are required to understand the community-wide hazards associated with fires arising from flammable gases and hazards that could result from a toxic chemical release. Furthermore, it is necessary for emergency managers to collaborate with regional laboratories and state and federal public health agencies to identify the agent, to treat the victims, and to decontaminate the incident site (Lindell et al. 2006). In response to chemical emergencies, EPA and NOAA developed a modeling program called Areal Locations of Hazardous Atmospheres (ALOHA) that is designed to evaluate releases of hazardous chemical vapors and predict threat zones associated with hazardous chemical releases such as toxic gas clouds, fires, and explosions (see https://www.epa.gov/cameo/what-cameo-software-suite#ALOHA). The scenarios and threat zones can be displayed on MARPLOT, which is a GIS-based mapping platform for this system (see https://response.restoration.noaa.gov/marplot).

Research on Toxic Release Inventory (TRI) and Superfund Sites

Bowen and others (1995) utilized 1990 census tract data and GIS tools to study the status of environmental inequity in the state of Ohio. They discovered that there existed high correlations between the distributions of minority populations and the locations of toxic release inventory (TRI) facilities within the state of Ohio, especially concentrated in urban areas (Bowen et al. 1995). Furthermore, Glickman and Hersh (1995) analyzed differential levels of risk from TRI facilities in the Pittsburgh area and found that three groups were at higher risks than the general population: all blacks, all poor, and the elderly.

Stretesky and Hogan (1998) investigated the spatial relationship between Superfund sites and the racial and socioeconomic characteristics in order to detect the extent of environmental injustice in the state of Florida. Their research suggested that African-Americans and Latinos tended to reside near Superfund sites, but indicators of income and poverty were not significantly correlated with the locations of Superfund sites. Maranville and others (2009) utilized an area-apportionment method, GIS tools, and statistical techniques to determine the correlation between the demographic and socioeconomic characteristics of a community and its proximity to the Superfund sites in Illinois. They discovered that the proportions of minority populations within 1-, 2-, and 5-mile radii buffer zones of Superfund sites were significantly higher than those outside the buffer zones. Their investigations suggested that race, instead of class, was the major cause of environmental injustice (Maranville et al. 2009).

Conclusion

Even though we cannot control all natural and technological hazards, we can still utilize GIS tools to identify potential hazard exposures, map social vulnerability, and apply protective actions for saving our lives. As Tomaszewski (2014) noted, hazard mitigation for GIS often requires interdisciplinary collaborations in earth science, sociology, and environmental science, and those mitigation activities must be guided by the underlying scientific principles, processes, and vulnerabilities. Indeed, using GIS not only allows governmental agencies and institutions to analyze and address issues of emergency management but also demonstrates a great way to promote risk communications with the public.

Cross-References

- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Preparedness and Planning
- ▶ Federal Emergency Management Agency
- ▶ Human-made Disasters: Toxic Waste and Residences
- ▶ Natural Hazards

References

Baker, E. J. (1991). Hurricane evacuation behavior. *International Journal of Mass Emergencies and Disasters, 9*, 287–310.

Blong, R. J. (1984). *Volcanic hazards: A sourcebook on the effects of eruptions*. Orlando: Academic.

Bowen, W. M., Salling, M. J., Haynes, K. E., & Cyran, E. J. (1995). Toward environmental justice: Spatial equity in Ohio and Cleveland. *Annals of the Association of American Geographers, 85*, 641–663.

Drabek, T. E. (1991). Introduction. In T.E. Drabek & G.J. Hoetmer (eds.) *Emergency management: Principles and practice for local government* (pp. xvii–xxxiv). Washington DC: International City Management Association.

Glickman, T. S., & Hersh, R. (1995). *Evaluating environmental equity: The impacts on industrial hazards on selected social groups in Allegheny County, Pennsylvania*. Discussion paper 95-13. Washington, DC: Johns Hopkins Press/Resources for the Future.

Gregg, C. E., Houghton, B. F., Johnston, D. M., Paton, D., & Swanson, D. A. (2004). The perception of volcanic risk in Kona communities from Mauna Loa and Hualalai volcanoes, Hawaii. *Journal of Volcanology and Geothermal Research, 130*, 179–196.

Islam, T., & Ryan, J. (2015). *Hazard mitigation in emergency management* (1st ed.). Waltham: Butterworth-Heinemann.

Johnston, D. M., Bebbington, M. S., Lai, C. D., Houghton, B. F., & Paton, D. (1999). Volcanic hazard perceptions: Comparative shifts in knowledge and risk. *Disaster Prevention and Management: An International Journal, 8*, 118–126.

Lindell, M. K., & Hwang, S. N. (2008). Households' perceived personal risk and responses in a multihazard environment. *Risk Analysis, 28*, 539–556.

Lindell, M. K., Lu, J. C., & Prater, C. S. (2005). Household evacuation decision making in response to Hurricane Lili. *Natural Hazards Review, 6*, 171–179.

Lindell, M. K., Prater, C. S., & Perry, R. W. (2006). *Fundamentals of emergency management*. Emmitsburg: FEMA Emergency Management Institute.

Maranville, A. R., Ting, T.-F., & Zang, Y. (2009). An environmental justice analysis: Superfund sites and surrounding communities in Illinois. *Environmental Justice, 2*, 49–56.

Palm, R., Hodgson, M., Blanchard, R. D., & Lyons, D. (1990). *Earthquake insurance in California*. Boulder: Westview Press.

Peacock, W. G., Brody, S. D., & Highfield, W. (2005). Hurricane risk perceptions among Florida's single family homeowners. *Landscape and Urban Planning, 73*, 120–135.

Star, J., & Estes, J. E. (1990). *Geographic information system: An introduction*. Upper Saddle River: Prentice Hall.

Stretesky, P., & Hogan, M. (1998). Environmental justice: An analysis of superfund sites in Florida. *Social Problems, 45*, 268–287.

Tomaszewski, B. (2014). *Geographic information systems (GIS) for disaster management*. Boca Raton: CRC Press.

Waugh, D. (2002). *Geography: An integrated approach*. Cheltenham: Nelson Thornes.

Wei, H.-L., & Lindell, M. K. (2017). Washington households' expected responses to lahar threat from Mt. Rainier. *International Journal of Disaster Risk Reduction, 22*, 77–94.

Zhang, Y., Hwang, S. N., & Lindell, M. K. (2010). Hazard proximity or risk perception? Evaluating effects of natural and technological hazards on housing values. *Environment and Behavior, 42*, 597–624.

Further Reading

Abdalla, R. (2016). Evaluation of spatial analysis application for urban emergency management. *SpringerPlus, 5*, 2081. https://doi.org/10.1186/s40064-016-3723-y.

Kataoka, M. (2007). *GIS for homeland security*. Redlands: ESRI Press.

Pine, J. C. (2018). *Technology and emergency management* (2nd ed.). Hoboken: Wiley.

H

Hazardous Environmental Effects

Denise D. P. Thompson
Department of Public Management, John Hay College of Criminal Justice, The City University of New York, New York, NY, USA

Keywords
Environmental hazards · Health effects · Chemical, Biological, Radiological, Technological · Physical · Flint

Definition

Hazardous environments are those where one or a group of toxic chemical, biological, radiological, technological, or physical agents in the environment may kill or negatively impact the health of those exposed to them, particularly children (World Health Organization n.d.).

Introduction

Our quality of life and years of healthy living is dependent on maintaining healthy environments. Globally, around 23% of all deaths and over a quarter (26%) of deaths among children 5 years and younger are due to environmental hazards (Department of Health and Human Services 2014). As far as environmental hazards are concerned, we live in a world of contradictions. As human beings we require clean environments to live a good quality of life, but in our daily living, we are the principal drivers of hazardous environments by the way we live and work.

For instance, whether on purpose or because of a lack of knowledge, lapses in judgment or malfunction in technical systems or in the built environment often result in harmful environmental conditions (Department of Health and Human Services 2014). We release hazardous environmental pollutants in the air, waterways, and drinking water supply. Pollutants such as pesticides, Chlorofluorocarbons (CFCs), secondhand tobacco smoke, industrial and home chemicals contaminate the atmosphere. Chemicals including lead, polychlorinated biphenyls, microbes, and suspended matter contaminated drinking water, and toxic waste like sludge contaminate the sea, rivers, and lakes. These substances have adverse effects on our health. In addition, naturally occurring factors including climate change, earthquakes, landslides, ozone build-up put our life and health in danger (Department of Health and Human Services 2014).

Chemical Hazards and Their Effects

Chemical, environmental hazards can result in short and long consequences to those exposed to them (World Health Organization Institute n.d.).

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

These agents include nerve agents that can enter the body through the skin or lungs and affect the nervous system (e.g., sarin, VX, and VR), and systemic agents such as hydrogen cyanide that enter the bloodstream either directly or indirectly and are transported throughout the body (Ganesan et al. 2010). Also, respiratory agents including chlorine are inhaled and can cause damage to the lungs. Moreover, blister agents like mustard gas damage the skin (Ganesan et al. 2010).

Depending on the severity of the exposure, impacts may include temporary illness or injury, permanent medical conditions, or death. For instance, Grandjean et al. (2007) found that reproductive health, as well as embryonic, fetal, and infant development, is susceptible to chemical hazards. Toxic exposures to chemical pollutants during human developmental stages can cause disease and disability not only in infants and children but across the entire human life cycle. In adults, chemical hazard exposure is linked to spontaneous abortion, congenital malformations, lowered birthweight, physical or mental illnesses that either remain or only become evident, months or years of exposure (WHO Institute n.d.; Grandjean et al. 2007). Some chemical agents have been strongly linked to cancer in humans (WHO Institute n.d.). Short-term effects include stomachaches, rashes, headaches, and nausea (WHO Institute n.d.). Chemical agents can enter the digestive system via contaminated food or drinking water, by hand to mouth contact from touching contaminated surfaces, or by swallowing respiratory mucus containing accumulated larger aerosol particles in the nose, throat, and upper airways (WHO Institute n.d.).

Biological Hazards and Their Effects

Biological hazards are disease-causing microorganisms and pathogens that can multiply within a human host and cause an infection (Bacon and Sofos 2003). These agents include bacteria, viruses, fungi, other microorganisms that could cause grave injury to individuals or a group because many microbes reproduce rapidly and require minimal resources to survive (OSHA n.d.). Infections typically occur because of airborne exposure through inhalation (e.g., with Bacillus species, anthrax spores) and skin contact with contaminated surfaces (as with MRSA and Staph). Some biological agents can be spread from one individual to another (Ebola hemorrhagic fever [EHF]) (OSHA n.d.). Contamination is also possible through ingestion of contaminated food or water as is the case with *E. coli*, which causes gastrointestinal infection (OSHA n.d.).

Radiological Hazards and Their Effects

Radiation is energy released from light, heat, sound, and charged particles that can cause direct or indirect damage to the body (Alameda County Public Health Department 2013). We experience some level of radiation exposure during the ordinary course of everyday living (e.g., sunshine). We are also exposed to human-made radiation (from microwave ovens) and medical sources (from x-rays), which in sufficiently large dosage can cause unhealthy health effects. Large amounts of radiation can occur in places such as a nuclear power plant accident or a terrorist attack (Alameda County Public Health Department 2013). Radiation exposure and radioactive contamination can occur if radioactive materials are released into the environment because of an accident, an event in nature (e.g., an earthquake), or an act of terrorism (CDC 2018). Such a release could expose people and contaminate their surroundings and personal effects. Radioactive contamination can occur when radioactive material is deposited on or in an object or a person.

Radiological hazards can contaminate drinking-water sources because of the mining industry and hydraulic fracturing or radionuclides from the medical or industrial enterprise that use radioactive materials (World Health Organization n.d.). Radioactive materials released into the atmosphere can cause air, water, surfaces, soil, plants, buildings, or even people, or animals to become contaminated (CDC 2018). There are some types of radioactive materials that stay in the body and are deposited in different organs.

Others are eliminated from the body in blood, sweat, urine, and feces (CDC 2018).

A contaminated person has radioactive materials on or inside their body. When radioactive materials enter the body either through an open wound, swallowing, or breathing or are absorbed through the skin, it is referred to as internal contamination (CDC 2018). Alternately when contact is external to a person's body such as with radioactive dust, powder, or liquid, which meets a person's skin, hair, or clothing, it is referred to as external contamination (CDC 2018). External contamination can become contamination internally if radioactive material gets into their bodies from these sites (CDC 2018).

Those exposed to large doses of radiation can display signs of acute radiation syndrome (ARS), or radiation sickness, a severe short-term illness whose symptoms include nausea, vomiting, headache, and diarrhea (CDC 2018). After the initial symptoms, a person usually looks and feels healthy for a period. However, then he or she becomes ill again often showing variable symptoms and severity that change over time depending on the radiation dosage received (CDC 2018). If death occurs, it is usually from the destruction of the person's bone marrow, which then leads to infections and internal bleeding (CDC 2018). Other less severe symptoms of radiation contamination include loss of appetite, fatigue, fever, nausea, vomiting, diarrhea, and possibly even seizures and coma. The amount of radiation an individual can absorb is called the radiation dose (CDC 2018). The lower the dose, the more likely it is for the individual to survive.

Technological Hazards and Their Effects

Hazardous environmental effects because of technological hazards are human-caused events that negatively impact people, their livelihood, and their property. Technological hazards are usually the result of increased opportunities for human error inherent in the use of harmful materials such as hazardous waste, sloppy craft, machine failure, or failure in routine monitoring (FEMA n.d.).

Often, little or no warning precedes technological incidents (FEMA n.d.). In many cases, victims may not know they have been affected until many years later. For example, health problems caused by hidden toxic waste sites – like that at Love Canal, near Niagara Falls, New York – surfaced years after initial exposure (FEMA n.d.). For example, A series of reports on the health effects of the Love Canal landfill disaster including a study commissioned by the NYS Department of Health in 2008, nearly 40 years after the disaster, found excess lung cancer kidney, bladder, and other cancers among those exposed to chlorinated benzenes and aniline compounds (Division of Environmental Health Assessment Center for Environmental Health 2008). Moreover, the rates of congenital malformations exceeded those for the general population and indicated potential chemical exposure as a child (Division of Environmental Health Assessment Center for Environmental Health 2008).

Technological hazards have the potential to happen suddenly and impact a low to moderate number of people like the Concorde airline crash in July 2000 that killed over 100 people, or the pedestrian bridge collapsed at Florida International University in Miami on March 15, 2018, that killed eight people. Others have the potential to impact large populations severely and to go on for extended periods as in the Three Mile Island, Pennsylvania, nuclear plant accident in 1973. Among other things, that incident caused elevated cancer levels of those living within a 10-mile radius of the incident and halted the development of nuclear power industry for 30 years in the USA (see Amadeo 2018).

Physical Hazards and Their Effects

Physical agents are "[a]ny phenomenon that threatens, or causes damage and destruction to people's lives, livelihood, their property and communities" (Watson 2015) because of their geographic, social, and economic vulnerabilities. A natural hazard is one produced by environmental process such as storms, floods, earthquakes, and volcanic eruptions (Watson 2015). Therefore,

hazardous environments may result from naturally occurring phenomena such as crustal (tectonic) movement such as earthquakes and resultant hazards such as shaking, landslides, tsunami; lava flows, mudflows, pyroclastic, and ash fallout volcanic hazards; and types of the eruption and their products (Watson 2015). Moreover, mass movements that result from slope instability that causes avalanches, rock slides, rock falls, landslides, and associated hazards can cause physical threat to populations living in their paths. Further, atmospheric disturbances associated with tropical storms such as cyclones and tornadoes and related hazards including storm surges, coastal flooding, severe river floods, landslides, high winds, pressure imbalances may pose a physical threat to life, property, and livelihood of populations they impact (Watson 2015).

Physical hazards can cause sedimentation in the water supply. Sediments and particulates can also include pipe materials, pipe liner materials, sloughed biofilms, or iron and manganese films (Watson 2015). Suspended or resuspended sediments can contain toxic chemicals or can have pathogens attached and can co-transport other hazards (World Health Organization n.d.), leading to poor ground and surface water quality. Concerns are increasing globally about both drinking water and recreational waters and the effects of chemical, biological, radiological, and physical agents on it (Watson 2015).

The Case of Hazardous Environmental Effects from Drinking Water in Flint, Michigan

The 2014–2016 water crisis in the city of Flint presents an example of the confluence of chemical, biological, technological factors resulting in harmful environmental effects to a group of people in the United States. The case is deemed one of the most significant public health failures of modern water supply in the USA (See Butler et al. 2016). It garnered public outcry and resulted in action at federal, state, and local levels, but not before over 8000 children were estimated to have been impacted by high lead levels in the Flint water supply.

The aging water distribution system in Flint contained a high percentage of lead pipes and lead plumbing, with estimates of lead service lines ranging from 10% to 80% (Hanna-Attisha et al. 2016; Jurkiewicz 2016). This situation along with cost-cutting measures during the 2010 recession in the United States created conditions where sections of Flint's population were exposed to detrimental effects of contaminated water. In its cost-saving efforts, the city decided to change water sources from the Detroit to the more corrosive Flint River. This decision proved to be a mistake.

Testing between October and December 2015 revealed that blood lead levels (BLLs) in children increased significantly. In the areas where lead levels in the water were at their highest, the BLLs in tested children increased by about 2.5 times previous levels (CNN 2018). Approximately 6% of the samples provided by Flint residents in January 2016 contained lead levels well over 15 parts per billion (ppb), which surpasses the federal action level (Hanna-Attisha et al. 2016; CNN 2018). The highest lead levels measured exceeded 5000 ppb. In some premises, both lead and copper levels were at critically high levels (CNN 2018). The aging Flint water distribution system contained a high percentage of lead pipes and lead plumbing, with estimates of lead service lines ranging from 10% to 80% (Hanna-Attisha et al. 2016; Jurkiewicz 2016).

In September 2014 three water alerts were issued, and another three boil water alerts were issued in a 22-day period in August 2015 as the bacterium *E. coli* had exceeded regulatory limits (Jurkiewicz 2016). As a result, the dosage of the disinfectant chlorine was increased, which resulted in violations for total trihalomethanes (TTHMs), which is cancer causing and a byproduct of the reaction of chlorine with the naturally occurring organic matter.

Drinking water that is inadequately treated or disinfected or that passes through an improperly maintained distribution system may also pose a health risk. Drinking water need only contain small amounts of some contaminants (copper, Mercury, Copper, lead) to be harmful if consumed (EPA 2017). Water quality concerns are increasing globally and include concerns for drinking as well as recreational water.

Lead is a well-established threat to children and pregnant women, but the Safe Drinking Water Act does not regulate lead in drinking water. Instead, the Clean Water Act (CWA) regulates lead in drinking water. The CWA prohibits anyone from discharging pollutants, including lead, through a point source into a water of the United States unless they have a National Pollutant Discharge Elimination System (NPDES) permit (EPA 2016; see also the US Lead and Copper Rule). Copper and lead enter our drinking water primarily through plumbing materials (EPA 2016). Exposure to lead and copper is potentially deadly and may cause health problems ranging from stomach distress to brain damage (EPA 2016). Lead exposure in children may result in anemia, kidney damage, colic, muscle weakness, and brain damage (Butler et al. 2016). Exposure to the fetus during pregnancy can result in fetal death, premature delivery, low birth weight, and lower intelligence in later childhood (Butler et al. 2016).

Regulating Hazardous Environments

In the United States, regulation of hazardous environmental effects occurs at the local, state, and federal levels. For instance, in the case of drinking water, the Safe Drinking Water Act is the chief federal law that regulates our potable water supplies. The Environmental Protection Agency sets drinking water standards and oversees states, municipalities, and water suppliers who implement those standards (EPA 2018). The EPA supports municipal wastewater treatment plants and participates in pollution prevention efforts meant to protect watersheds and other sources of drinking water (EPA 2018).

The Safe Drinking Water Act sets up multiple barriers against pollution and ensures the highest quality of drinking water. These barriers include source water protection, treatment, distribution system integrity, and public information (EPA n.d.). Public water systems must ensure that contaminants in drinking water do not exceed the stipulated standards (EPA n.d.). When the water quality does not meet these standards, it is the water supplier's responsibility to notify its customers (EPA n.d.). Many water suppliers now are also required to prepare annual reports for their customers, who are expected to work with local water suppliers to set priorities, make decisions on funding and system improvements, and establish programs to protect drinking water sources (EPA n.d.).

Besides, every state must assess its drinking water sources (rivers, lakes, reservoirs, springs, and groundwater wells) under the Source Water Assessment Program to identify potential contamination sources and determine how susceptible the sources are to these threats (EPA n.d.). Moreover, per the Stage1 Disinfectants and Disinfection Byproducts Rule and the Interim Enhanced Surface Water Treatment Rule, the EPA is required to strengthen protection for microbial contaminants (EPA n.d.).

Conclusion

Maintaining healthy environments is central to our quality of life and years of healthy living more generally. Often poor critical public infrastructure, poor decision-making, inadequate regulatory oversight, human error, and financial vulnerability lead to hazardous environmental conditions and unhealthy effects. The water crisis in Flint, Michigan, is just one example of the increasing hazardous health effects from environmental contamination occurring globally. Human beings need to reconsider how we relate to the environment and the impacts that our actions on it. Public policy and their enforcement have worked to regulate our behavior regarding the use and abuse of our natural environment, but even the policies must incorporate a fundamental reconsideration of how human beings interact with their environment in a more systemic and sustainable way.

Cross-References

▶ Emergency Management: Recent Incidents That Contributed to Changes in Emergency Management Legislation and Procedures

▶ Emergency Management: Working with Vulnerable Populations

References

Alameda County Public Health Department. (2013). Facts about chemical and radiological agents. Retrieved from http://www.acphd.org/phep/health-and-safety/chemical-and-radiological-agents.aspx

Bacon, R. T., & Sofos, J. N. (2003). Characteristics of biological hazards in foods. In *Food safety handbook* (pp. 157–195). Hoboken: Wiley-Interscience.

Butler, L. J., Scammell, M. K., & Benson, E. B. (2016). The Flint, Michigan, water crisis: A case study in regulatory failure and environmental injustice. *Environmental Justice, 9*(4), 93–97.

CDC. (2018). Radiological contamination: Contamination vs. exposure. Retrieved from https://emergency.cdc.gov/radiation/contamination.asp

CNN. (2018). Flint water crisis fast facts. Accessed at https://www.cnn.com/2016/03/04/us/flint-water-crisis-fast-facts/index.html

Department of Health and Human Services. (2014). Environmental health. In HealthyPeople.gov, Office of Disease Prevention and Health Promotion. Retrieved from https://www.healthypeople.gov/2020/topics-objectives/topic/environmental-health

Division of Environmental Health Assessment Center for Environmental Health. (2008). Love canal follow-up health study. Prepared for the New York State Department of Health for the U.S. Department of Health and Human Services Agency for Toxic Substances and Disease. Retrieved from https://www.health.ny.gov/environmental/investigations/love_canal/docs/report_public_comment_final.pdf

Environmental Protection Agency. (2016). Drinking water lead and copper rule historical documents. Retrieved from https://www.epa.gov/dwreginfo/drinking-water-lead-and-copper-rule-historical-documents#rule

Environmental Protection Agency. (2017). Drinking water contaminants – Standards and regulations. Accessed at https://www.epa.gov/dwstandardsregulations

Environmental Protection Agency. (2018). Summary of the Clean Water Act, PDF of CWA (234 pp, 1 MB), *33 U.S.C. §1251 et seq*. (1972). Retrieved from https://www.epa.gov/laws-regulations/summary-clean-water-act

Environmental Protection Agency. (n.d.). Understanding the safe drinking water act: The safe drinking water act 1974–2004. Retrieved from https://www.epa.gov/sites/production/files/2015-04/documents/epa816f04030.pdf

FEMA. (n.d.). Technological hazards. Retrieved from https://www.fema.gov/pdf/areyouready/technohazards.pdf

Ganesan, K., Raza, S. K., & Vijayaraghavan, R. (2010). Chemical warfare agents. *Journal of Pharmacy & Bioallied Sciences, 2*, 166–178.

Grandjean, P., Bellinger, D., Bergman, A., Cordier, S., Davey-Smith, G., Brenda Eskenazi, B., Gee, D., Gray, K., Hanson, M., Van Den Hazel, P., Heindel, J. J., Heinzow, B., Hertz-Picciotto, I., Hu, H., Huang, T. T.-K., Jensen, T. K., Landrigan, P. J., McMillen, I. C., Murata, K., Ritz, B., Schoeters, G., Skakkebæk, N. E., Skerfving, S., & Weihe, P. (2007). The Faroes statement: Human health effects of developmental exposure to chemicals in our environment. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/j.1742-7843.2007.00114.x

Hanna-Attisha, M., LaChance, J., Sadler, R. C., & Champney Schnepp, A. (2016). Elevated blood lead levels in children associated with the Flint drinking water crisis: A spatial analysis of risk and public health response. *American Journal of Public Health, 106*(2), 283–290.

Jurkiewicz, C. (2016). Flint, Michigan. *Public Integrity, 18*(3), 233–236. https://doi.org/10.1080/10999922.2016.1152760.

Occupational Safety and Health Administration. (n.d.). Biological agents. Retrieved from https://www.osha.gov/SLTC/biologicalagents/

Watson, M. (2015). Hazardous environments. Retrieved from https://maxwatsongeography.wordpress.com/section-a/hazardous-environments/

World Health Organization Institute. (n.d.). Public health response to biological and chemical weapons – WHO guidance. pp. 25–52. Retrieved from http://www.who.int/csr/delibepidemics/chapter3.pdf

Further Reading

Amadeo, K. (2018, updated). Three Mile Island nuclear accident facts, impact, and status today. The balance. Accessed at https://www.thebalance.com/three-mile-island-nuclear-accident-facts-impact-today-3306337

Field, W. (2005). Three Mile Island epidemiologic radiation dose assessment revisited: 25 years after the accident. *Radiation Protection Dosimetry, 113*(2), 214–217.

Fleming, R., Baum, A., Gisriel, M. M., & Gatchel, R. J. (1982). Mediating influences of social support on stress at Three Mile Island. *Journal of Human Stress, 8*(3), 14–23.

Masten, S. J., Davies, S. H., & Mcelmurry, S. P. (2016). Flint water crisis: What happened and why? *Journal-American Water Works Association, 108*(12), 22.

Needham, L. L., & Sexton, K. E. N. (2000). Introduction and overview: Assessing children's exposure to hazardous environmental chemicals: An overview of selected research challenges and complexities. *Journal of Exposure Science and Environmental Epidemiology, 10*(S6), 611.

Office of the Governor. (2016). Flint Water Advisory Task Force, final report. Retrieved from https://www.michigan.gov/documents/snyder/FWATF_FINAL_REPORT_21March2016_517805_7.pdf

HAZMAT

Michael K. Lindell
Department of Urban Design and Planning, Institute for Hazards Mitigation Planning and Research, University of Washington, Seattle, WA, USA

Keywords
Extremely Hazardous Substance (EHS) · Inhalation hazard · Vulnerable zone (VZ) · Level of concern (LOC) · Atmospheric dispersion

Definition

Hazardous materials are substances "capable of posing unreasonable risk to health, safety and property" (949 CFR 171.8).

Introduction

Hazardous materials (commonly known as *hazmat*) are regulated by a number of federal agencies, including the Department of Transportation (DOT), Environmental Protection Agency (EPA), Nuclear Regulatory Commission (NRC), and Occupational Safety and Health Administration of the Department of Labor. In addition, the Coast Guard and Federal Emergency Management Agency of the Department of Homeland Security have responsibilities for emergency response to hazmat incidents. Because these agencies have different responsibilities, they have correspondingly different definitions of hazmat.

Hazmat regulations cover a wide range of issues, but this entry focuses on emergency response to unplanned releases that pose a threat to the general public. Thus, this entry does not address the management of chronic chemical pollution under the Toxic Substances Control Act and Pollution Prevention Act; hazardous waste under the Resource Conservation and Recovery Act; hazmat cleanup under the Comprehensive Environmental Response, Compensation, and Liability Act; protection of workers engaged in hazardous waste operations and emergency response or oil spill preparedness and response under the Oil Pollution Act; and the Spill Prevention, Control, and Countermeasure Rule.

Emergency response to hazmat incidents has long been recognized to be a responsibility of local emergency responders in public safety agencies such as fire and police departments. These agencies can provide a satisfactory response to minor incidents, especially when they follow the DOT's *Emergency Response Guidebook* (DOT 2016) in making protective action decisions. However, the 1984 toxic chemical release in Bhopal India called attention to the need for comprehensive planning involving cases of major releases. Thus, the 1986 Emergency Planning and Community Right to Know Act (EPCRA, also known as Title III of the Superfund Amendments and Reauthorization Act – SARA Title III) required each state to establish a State Emergency Response Commission (SERC) and Local Emergency Planning Districts, each of which would have a Local Emergency Planning Committee (LEPC).

LEPCs are expected to work with local facilities that are storing more than the maximum allowable amount of chemicals designated by the EPA as extremely hazardous substances (EHSs). Specifically, this collaboration requires identifying the EHSs stored onsite and the quantities of those substances. In addition, it requires computing the radius of vulnerable zones (VZs) around the facilities and developing plans for responding to releases of those EHSs (NRT 1988, 2001). In the longer term, local jurisdictions should promote safe land use practices to ensure that high-density residential and commercial land uses are located outside the VZs for fixed-site facilities and are adequately separated from transportation routes where high volumes of hazmat are carried. High priority should be given to facilities, such as schools, hospitals, and nursing homes, that house vulnerable population segments lacking physical mobility or ready access to evacuation vehicles (see ▶ "Emergency Management: Evacuations"). Local jurisdictions

should also work with energy utilities to encourage the reduction of air infiltration in new structures and retrofits of existing structures because this will save energy in the short run and also support sheltering in-place during a hazmat release (see ▶ "Emergency Management: Shelter In-Place").

Hazmat Release Sources

Planners typically expect to find hazmat produced, stored, or used at fixed-site facilities, such as petrochemical and manufacturing plants, but these materials are also found in warehouses (e.g., agricultural fertilizers and pesticides), water treatment plants (chlorine is used to purify the water), and breweries (ammonia is used as a refrigerant). Moreover, hazmat is transported from one location to another by a variety of modes – ship, barge, pipeline, rail, truck, and air. In general, the quantities of hazmat on ships, barges, and pipelines can be as large as is stored at many fixed-site facilities, but usually the amounts are smaller for other modes of transportation, decreasing in size from rail to truck to air. Small- to moderate-sized releases of hazardous materials at fixed-site facilities are occupational hazards but often pose little risk to public health and safety because exposure resides entirely within the facility boundaries. However, releases of this size during hazmat transportation can be a public hazard because passersby can easily enter the risk area and become exposed. The amount actually released is often much smaller than the total quantity available in the container, but prudence dictates that planning processes assume the plausible worst cast of complete release within a short period of time (e.g., 10 min in the case of toxic gases).

Hazardous Materials Classification

There are thousands of chemicals in commercial use, but they can be categorized into nine classes based on their chemical and physical properties.

Explosives

Explosives cause casualties and property damage by overpressure from atmospheric blast waves and flying debris. Destructive effects from quantities found in transportation can be felt as much as a mile (1.6 km) or more away from the incident site.

Flammable Gases

Flammable gases such as liquefied petroleum gas (LPG) can travel downwind after release until they reach an ignition source, such as the pilot light in a water heater or the ignition system in a car. At distances of 0.5 miles (0.8 km) or more, the gas cloud can erupt in a fireball that flashes back toward the release point. Explosive rupture of gas containers can launch fragments up to 1 mi (1.6 km), so evacuation out to this distance is advised if there is a fire.

Flammable Liquids

Flammable liquids, such as gasoline, present a similar threat as flammable gases, in that a volatile liquid (one that rapidly produces much vapor) can travel toward an ignition source and erupt in flames when an ignition source is reached. When a flammable liquid is dispersed on land, there should be a downwind evacuation of at least 0.2 mi (0.3 km). A flammable liquid that floats downstream on water could be dangerous at even greater distances. A fire should stimulate consideration of an evacuation of approximately 0.5 mi (0.8 km) in all directions.

Flammable Solids

Flammable solids are less dangerous than flammable gases or liquids because they do not disperse over such wide areas. A large spill requires a downwind evacuation of 300 ft (0.1 km), but a fire should produce an evacuation of 0.5 mi (0.8 km) in all directions.

Oxidizers and Organic Peroxides

These substances do not burn but are hazardous because they promote combustion. A large spill should prompt a downwind evacuation of 0.3 mi (0.5 km), and a fire should initiate an evacuation of 0.5 mi (0.8 km) in all directions.

Toxic Materials and Infectious Substances

Toxic (poisonous) materials are hazardous when inhaled into the lungs, ingested into the stomach by means of contaminated water or food, or absorbed through the skin. Of these exposure pathways, inhalation hazard is typically the greatest concern because high concentrations can kill in a matter of seconds. Moreover, chemical contamination of victims could pose problems for volunteers and professionals providing first aid and transporting victims to hospitals. These chemicals vary substantially in their volatility and toxicity, so protective action distances following a spill or fire during a transportation incident must be determined from the Table of Protective Action Distances in the *Emergency Response Guidebook*. Protective action distances for releases from fixed-site facilities are more complex and are addressed below. Infectious substances have rarely been significant to date, but the potential for large-scale terrorist attacks should be of concern to emergency planners.

Radioactive Materials

With the exception of nuclear power plants, the planning for which is supported by guidance from NRC (1980), releases of radioactive materials are likely to involve only small quantities. Nevertheless, even a few grams of a lost radiographic source for industrial or medical X-rays can generate a high level of public concern. Here also, the recently recognized threat of terrorist attack from a "dirty bomb" that uses a conventional explosive to scatter radioactive material over a wide area deserves planners' attention because of the potential for long-term contamination of central business districts. A large spill should prompt a downwind evacuation of approximately 300 ft (0.1 km), and a fire should initiate an evacuation of approximately 0.2 mi (0.3 km) in all directions.

Corrosive Materials

Corrosive materials, which can be either acidic or alkaline, cause chemical burns, but the substances in this class that are most frequently used and transported are not highly volatile. Thus, the geographical area affected by a spill is likely to be no greater than approximately 300 ft (100 m) unless the container is involved in a fire or the hazmat enters a waterway (e.g., via storm sewers). These chemicals vary substantially in their volatility and toxicity, so evacuation distances following a spill or fire must be determined from the Table of Protective Action Distances in the *Emergency Response Guidebook*.

Miscellaneous Dangerous Goods

This class comprises a diverse set of materials such as air bags, certain vegetable oils, polychlorinated biphenyls (PCBs), and white asbestos. Materials in this category are low to moderate fire or health hazards to people within 30–80 ft (10–25 m).

Airborne Hazmat Dispersion

The spread of an airborne release is defined by the hazmat's chemical and physical characteristics, its release characteristics, the topographic conditions in the release area, and the meteorological conditions at the time of the release. A hazmat's chemical and physical characteristics are its volatility (the rate at which the chemical becomes airborne per unit of time), buoyancy (whether it tends to flow into low spots because it is heavier than air), toxicity (the biological effect due to cumulative dose or peak concentration), and physical state – whether it is a solid, liquid, or a gas at ambient temperature and pressure.

Release characteristics are defined by the chemical's temperature and pressure in relation to ambient conditions, its quantity (measured by the total weight of the hazmat released), its release rate (in pounds per minute), and the surface area of the spilled pool if the substance is a liquid. Temperature and pressure are important because the rate at which the chemical disperses in the atmosphere increases when these parameters exceed ambient conditions. The release rate is important because it determines the concentration of the chemical in the atmosphere. Specifically, a release rate at the high end puts a large volume of

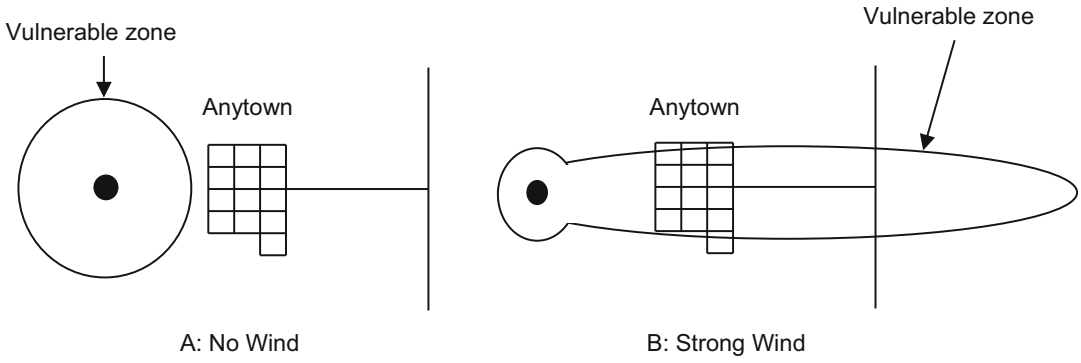
chemical into a given (limited) volume of air, thus increasing its concentration (the amount of chemical divided by the volume of air in which it is contained).

Topographical conditions relevant to liquid spills or dense gases are the slope of the ground and the presence of depressions. Steep slopes allow a liquid to rapidly move away from the location of the spill. Both flat slopes and depressions decrease the size of a liquid pool's surface area and, in turn, reduces the rate at which vapor is generated from it. Thus, hazmat facilities erect permanent dikes around chemical tanks to confine spills in case the tanks leak and hazmat responders build temporary dikes around spills for the same reason. Topographical characteristics also affect the dispersion of a chemical release within the atmosphere. Hills and valleys are land features that channel the wind direction and increase wind speed at constriction points – for example, where a valley narrows and causes wind speed to increase due to a "funnel" effect. Forests and buildings are rough surfaces that increase turbulence in the wind field, causing greater vertical mixing that dilutes the chemical's concentration in the atmosphere. By contrast, water bodies are smooth surfaces that produce minimal wind turbulence, thus allowing the hazmat to maintain a high concentration at ground level where people inhale it.

The meteorological conditions of concern during a hazmat release are wind direction, wind speed, and atmospheric stability. The effect of wind speed on atmospheric dispersion can be seen in Fig. 1, which shows a release dispersing uniformly in all directions when there is no wind (Panel A). Thus, any plume isopleth (contour of constant chemical concentration) for this chemical is a circle. The nearby town lies outside the plume so its inhabitants would not need to take protective action. However, Panel B describes the situation in which there is a strong wind, so a plume isopleth for this case is an ellipse. In this case, the nearby town lies inside the plume so people there would need to take protective action.

As Table 1 indicates, atmospheric stability can vary from Class A through Class F. Class A, the most unstable condition, occurs during strong sunlight (e.g., midday) and light wind. This dilutes the released chemical by mixing it into a larger volume of air. Class F identifies the most stable atmospheric conditions, which take place during clear nighttime hours when there is a light wind. These conditions have very little vertical mixing, so the released chemical remains highly concentrated at ground level.

It is important to recognize that, at some times, meteorological characteristics can remain stable for many days but, at other times, can change from 1 h to the next. Figure 2, which Lindell et al. (2006) adapted from McKenna (2000), displays the wind direction at each hour during the day of the 1979 accident at the Three Mile Island nuclear power plant in terms of the orientation of an

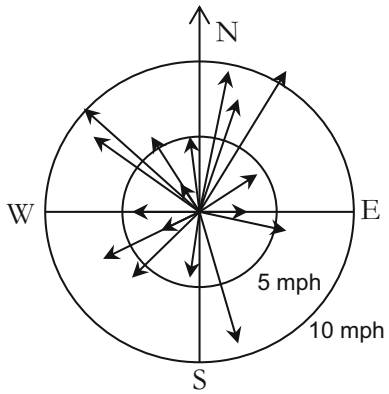


HAZMAT, Fig. 1 Effects of wind speed on plume dispersion. (From Lindell et al. 2006)

HAZMAT, Table 1 Atmospheric stability classes. (From FEMA/DOT/EPA n.d.)

	Strength of sunlight			Nighttime conditions	
Surface wind speed (mph)	**Strong**	**Moderate**	**Slight**	**Overcast ≥50%**	**Overcast <50%**
<4.5	A	A-B	B	–	–
4.5–6.7	A-B	B	C	E	F
6.7–11.2	B	B-C	C	D	E
11.2–13.4	C	C-D	D	D	D
>13.4	C	D	D	D	D

A: Extremely Unstable Conditions
B: Moderately Unstable Conditions
C: Slightly Unstable Conditions
D: Neutral Conditions (heavy overcast day or night)
E: Slightly Stable Conditions
F: Moderately Stable Conditions



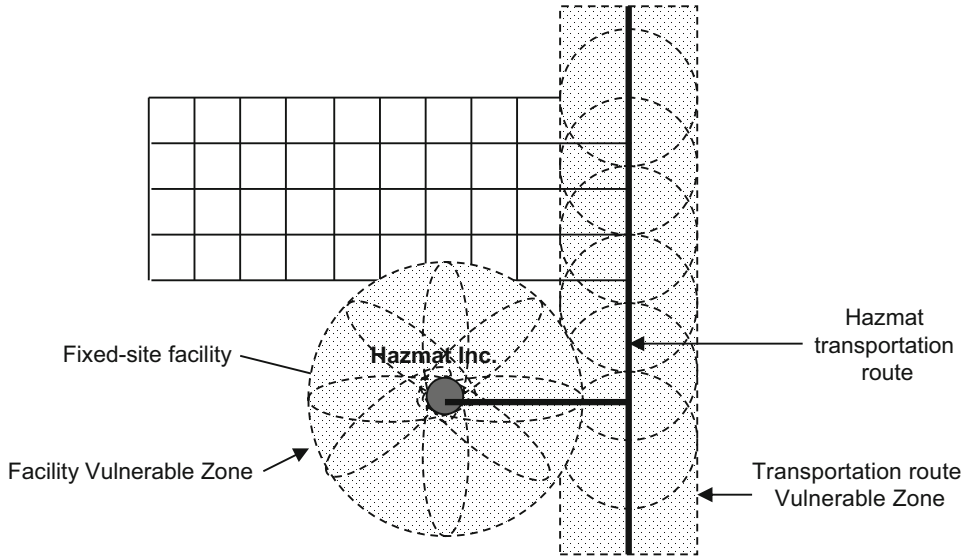
HAZMAT, Fig. 2 Wind Rose from 3 am to 6 pm on the 1st day of the 3 mile island nuclear power plant accident. (From Lindell et al. 2006)

arrow. Wind speed is indicated by the length of the arrow. The figure shows wind speed, and direction changed repeatedly during the course of the accident, so any recommendation to evacuate the area downwind from the plant would have referred to different geographic areas at different times during the day. This would have made evacuation notices extremely problematic because the time required to evacuate these areas would have taken many hours. Consequently, while the evacuation of one area was being implemented, the second order to evacuate in a very different direction would be issued, requiring simultaneous evacuations.

Hazmat Hazard Analysis: Fixed-Site Facilities

The process of identifying VZs around hazmat facilities begins by identifying dangerous chemicals (i.e., those that are threats because of their flammability, reactivity, or toxicity), their locations, and the quantities stored at those locations. Once the chemical inventory has been conducted, VZs can be computed using the data on the chemical's quantity available for release, the type of spill (liquid or gaseous), and the postulated release duration (e.g., 10 min) – all of which are combined to estimate the release rate. In addition, the VZ is defined by the chemical's toxicity, the assumed meteorological conditions (wind speed and atmospheric stability), and the terrain (urban or rural). Available methods for VZ computation are manual computations in the *Technical Guidance for Hazards Analysis* (USEPA 1987), desktop computations using *CAMEO/ALOHA* (FEMA, no date, see www.epa.gov/cameo), or online computations using *RMP*Comp* (www.epa.gov/rmp/rmpcomp).

Emergency planners can use the *Technical Guidance for Hazards Analysis* to calculate the size of the VZ for EHSs by identifying the number of pounds of hazmat in a tank or system of interconnected tanks (obtained from the facility operators) and the level of concern (LOC – the minimum concentration at which adverse health effects could occur – which is listed in an



HAZMAT, Fig. 3 Vulnerable zones around a fixed-site facility and transportation route. (From Lindell 2006)

appendix to the *Technical Guidance*). These data are used to enter one of four tables defined by the type of terrain (urban or rural) and atmospheric conditions at the time of the release (moderately stable or extremely stable). For example, the release of 800 lbs of chlorine (LOC = 0.0073) over a 10-min period from a water treatment plant located in a rural area during extremely stable atmospheric conditions and a wind speed of 3.4 mph (5.4 kph) would have a VZ radius of approximately 10 mi (16 km). If the plant were located in an urban area, the same scenario would result in a VZ radius of only about 1 mi (1.6 km) because the presence of buildings produces greater terrain roughness and, thus more vertical atmospheric mixing, than is found in rural areas.

Once the radii of the VZs for the different chemicals have been computed, these can be overlaid onto a map with the release point in the center of the circle and the radius drawn around it (see Fig. 3). The VZ around a fixed-site facility is a circle because a toxic chemical plume – which is usually elliptical in shape – could travel in any direction from the plant depending on wind direction. The VZs can then be used to identify areas within a jurisdiction that require hazard mitigation and emergency preparedness actions to protect the public health and safety, property, and the environment.

Hazmat Hazard Analysis: Transportation

Emergencies in hazmat transportation not only involve much smaller quantities of hazmat than at fixed-site facilities but, when they occur in populated areas, threaten local populations so quickly that emergency responders lack the time to perform the computations used for fixed-site facilities. Emergency planners should begin by identifying the highway, rail, water, and air routes through which hazardous materials are transported before an incident occurs. Once these routes have been identified, the number of tank trucks, railroad tank cars, and barges carrying each type of hazardous material can be counted in a *commodity flow study*. Information about hazardous materials transportation can be found on the DOT website (hazmat.dot.gov), and specific guidance for commodity flow studies is found at https://www.phmsa.dot.gov/technical-resources/hazmat-technical-resources/guidance-conducting-hazardous-materials-flow-studies. Once the

chemicals being transported have been identified, analysts can use the same procedures that were used for fixed-site facilities. A hazmat release can take place at any point along a transportation route, so its VZ is defined by a series of circles whose radius is calculated in the same way as for a fixed-site facility. Thus, the VZ for a transportation route forms a rectangle (see Fig. 3). The fixed-site facility and transportation route VZs can then be examined to identify areas of residential, commercial, and industrial land use (see Lindell et al. 2018, chapter 11, for an analysis of hazardous waste transportation to an incinerator).

If VZs for the transportation routes have not been identified before an incident occurs, local emergency responders need to search the incident scene for shipping papers, a numbered placard, or a placard with an orange numbered panel to obtain either the hazmat's name or its ID number so they can identify the correct section of the *Emergency Response Guidebook* (www.phmsa.dot.gov/hazmat/erg/erg2016-english). This document identifies these chemicals' potential hazards (fires, explosions, and toxic exposures), recommended response actions by firefighters and hazmat technicians, appropriate protective actions for emergency responders and the public, and recommended first aid measures for those who have received excessive exposures. For chemicals posing the greatest inhalation hazard, the *Emergency Response Guidebook* directs emergency responders to a Table of Initial Isolation and Protective Action Distances that should be used to select the appropriate protective action recommendations. These protective action distances are the equivalent of VZ radiuses for "small" and "large" spills during daytime and nighttime conditions. For a nighttime release of chlorine, the protective action distances would be 0.5 mi for a small release and 1.9 mi for a large release. Because the *Emergency Response Guidebook* classifies releases only as small or large, emergency planners should use the procedures in the *Technical Guidance for Hazards Analysis* or more advanced methods identified in the *Handbook of Chemical Hazard Analysis Procedures* wherever possible. In particular, the protective action distances in the *Emergency Response Guidebook* are *not* appropriate for use in computing VZs for fixed-site facilities.

Hazmat Hazard Analysis: Nuclear Power Plants

Exposure pathways for radiological materials are similar to those of toxic chemicals. Breathing air that is contaminated with radioactive materials can cause inhalation exposure, whereas eating food (e.g., unwashed local produce) or drinking liquids (e.g., water or milk) that is contaminated can cause ingestion exposure. Contamination also can enter the body through an open wound, such as a compound fracture, laceration, or abrasion, but radiological materials do not cause absorption exposures because they do not pass through the skin. However, because radiological materials release energy, they can produce exposures via direct radiation (also known as "shine") from a plume that is passing overhead. If the plume has a significant component of particulates, these might be deposited on the ground, vegetation, vehicles, or buildings, and the direct radiation from the deposited particulates would produce a continuing exposure. In this connection, it is important to recognize the distinction between irradiation and contamination. Irradiation involves the transmission of energy to a target that absorbs it, whereas contamination occurs when radioactive particles are deposited in a location within the body where they provide continuing irradiation.

The NRC conducted extensive analyses to define the emergency planning zones (EPZs) that should be designated around these facilities. These analyses led to the establishment of a 10-mile radius *plume inhalation EPZ* in which people might need to initiate protective actions to avoid inhalation exposure and direct radiation from a radioactive plume (NRC 1978). Protective actions within the 10-mile EPZ are expected to include sheltering, evacuation, and the use of potassium iodide. In addition, there is a 50-mile radius *ingestion pathway EPZ* in which authorities should prepare to monitor water, milk, and

food (especially leafy green vegetables) for contamination. Within the 50-mile radius, actions include bans on contaminated food and water (NRC 1980).

Conclusion

The *Emergency Response Guidebook* provides adequate guidance on the selection of protective actions for hazmat released during most transportation incidents. Such incidents can involve any one or more of a diverse set of chemicals, but the quantities tend to be small so protective actions are often – *but not always* – limited to the immediate vicinity of a release. However, incidents at fixed-site facilities can be much larger – sometimes affecting people 10 miles (16 km) or more downwind. Consequently, it is important for local emergency planners to know which facilities have hazmat and what are the quantities of hazmat that are stored at each facility. In addition, planners need to identify the VZs for each of the EHSs at these facilities and to develop emergency response plans that address protective actions such as evacuation or sheltering in-place.

Cross-References

- ▶ Emergency Management: Crisis Communication
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Preparedness and Planning
- ▶ Emergency Management: Shelter In-Place

Acknowledgments This research was supported by the National Science Foundation under Grants IIS-1540469, CMMI-1760766, and CMMI-1826455. None of the conclusions expressed here necessarily reflects views other than those of the author.

References

DOT – Department of Transportation, Transport Canada, Secretaría de Comunicaciones y Transportes. (2016). *Emergency response guidebook*. Washington, DC: DOT – Department of Transportation, Transport Canada, Secretaría de Comunicaciones y Transportes.

EPA – Environmental Protection Agency. (1987). *Technical guidance for hazards analysis: Emergency planning for extremely hazardous substances*. Washington, DC: EPA – Environmental Protection Agency.

FEMA/DOT/EPA – Federal Emergency Management Agency, Department of Transportation, and Environmental Protection Agency. (n.d.). *Handbook of chemical Hazard analysis procedures*. Washington, DC: FEMA/DOT/EPA – Federal Emergency Management Agency, Department of Transportation, and Environmental Protection Agency.

Lindell, M. K. (2006). Hazardous materials. In American Planning Association (Ed.), *Planning and urban design standards* (pp. 168–170). New York: Wiley.

Lindell, M. K., Prater, C. S., & Perry, R. W. (2006). *Fundamentals of emergency management*. Emmitsburg: Federal Emergency Management Agency Emergency Management Institute. www.training.fema.gov/EMIWeb/edu/fem.asp or hrrc.arch.tamu.edu/publications/books/.

Lindell, M. K., Murray-Tuite, P., Wolshon, B., & Baker, E. J. (2018). *Large-scale evacuation: The analysis, modeling, and management of emergency relocation from hazardous areas*. New York: Routledge.

McKenna, T. J. (2000). Protective action recommendations based upon plant conditions. *Journal of Hazardous Materials, 75*(2–3), 145–164.

NRC – Nuclear Regulatory Commission/Environmental Protection Agency. (1978). *Planning basis for the development of state and local government radiological emergency response plans in support of light water nuclear power plants* (NUREG-0396, EPA 520/1-78-016). Washington, DC: NRC – Nuclear Regulatory Commission/Environmental Protection Agency.

NRC – Nuclear Regulatory Commission/Federal Emergency Management Agency. (1980). *Criteria for preparation and evaluation of radiological emergency response plans and preparedness in support of nuclear power plants* (NUREG-0654, FEMA-REP-1, Rev.1). Washington, DC: NRC – Nuclear Regulatory Commission/Federal Emergency Management Agency.

NRT – National Response Team. (1988). *Criteria for review of hazardous materials emergency plans*. Washington, DC: NRT – National Response Team.

NRT – National Response Team. (2001). *Hazardous materials emergency planning guide*. Washington, DC: NRT – National Response Team.

Further Reading

Burke, R. (1997). *Hazardous materials chemistry for emergency responders*. Boca Raton: CRC Press.

DOT – Department of Transportation, Transport Canada, Secretaría de Comunicaciones y Transportes. (2016). *Emergency response guidebook*. Washington, DC: DOT – Department of Transportation, Transport Canada, Secretaría de Comunicaciones y Transportes.

Lesak, D. (1999). *Hazardous materials: Strategies and tactics*. Upper Saddle River: Brady/Prentice Hall.

Health Security: Securing Borders and Managing COVID-19

Michelle D. Miranda[1] and Marie-Helen Maras[2]
[1]Farmingdale State College, The State University of New York, Farmingdale, NY, USA
[2]Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Coronavirus · COVID-19 · Border security · Health security · National security · Pandemic · Quarantine

Definition

Health security: the branch of security concerned with the impact of factors that threaten health and human safety on a societal and global scale.

Introduction

In 2020, scientists and researchers are working around the clock to understand the cause and transmission of the 2019 Novel Coronavirus (2019-nCoV, or COVID-19) after it was first detected in Wuhan City, China, in late 2019. Despite the focus on an emerging and rapidly evolving situation, little has been done to address the implications of the spread of the coronavirus on national security. The 2020 reactive response to identifying and isolating known and suspected infected individuals has not proven effective, with cases of the coronavirus reported worldwide. While some countries have closed borders and applied travel restrictions, there appears to be no systematic, rapid response approach to doing so. Furthermore, the methods of screening passengers at travel hubs, such as airports, do not appear to be effectively screening out those individuals that could pose a national security risk. This entry presents an overview of the history and epidemiology of COVID-19 and evaluates the initial response and management of this pandemic in an effort to evaluate US national preparedness and encourage improved response to prevent future pandemic events.

Coronavirus: History and Epidemiology

The 2019 Novel Coronavirus, a betacoronavirus similar to MERS-CoV (Middle East Respiratory Syndrome) and SARS-CoV (Severe Acute Respiratory Syndrome), was first detected in Wuhan City, Hubei Province, China, in late 2019. This infectious disease is transmitted from animal to human and from human to human. Despite the Centers for Disease Control and Prevention (CDC) stating that much is unknown about the initial transmission of the virus, there is speculation that the initial transmission of COVID-19 occurred at a Chinese market selling live and dead animals, and sources of the transmission (*vector*) may have been a bat, a pangolin, or another species in that open-air market (Achenbach 2020).

As of the first half of 2020, the CDC stated on its website that "limited information is available to characterize the spectrum of clinical illness associated with [2019-nCoV]. No vaccine or specific treatment is available. . .and care is supportive" (CDC 2020a). Individuals infected with COVID-19 are described as having "flu-like" symptoms similar to those of most viral infections (e.g., fever, coughing, chest pain, and general body aches). Because these symptoms are similar to the flu, they can easily be dismissed and/or overlooked. Another problem with identifying and diagnosing infected individuals with COVID-19 is that the symptoms exhibited by infected individuals can vary between patients. Moreover, some patients have no identifiable symptoms and prior to any strategies implemented to slow the infection rate, such as social distancing and/or masks, passed the disease to multiple people who in turn passed it to others. This issue, coupled with the purported two-week incubation period of the virus, has made it challenging to effectively contain the virus. Efforts continue to be underway

to better understand the history and epidemiology of the virus.

National Security: Isolating Individuals, Closing Borders, and Restricting Travel

The ultimate objective of responses to outbreaks is to contain infectious diseases (Maras 2014). Historically, this was achieved by isolating infected individuals and/or placing them in quarantine, closing borders, and restricting travel (see, e.g., responses to the Ebola Virus, Maras and Miranda 2015). Governments worldwide responded in a similar manner to COVID-19. These responses, isolation and quarantine, border closings, and travel restrictions, are permitted by national and international law (see Maras and Miranda 2015 for more information).

Isolation and Quarantine

In response to the pandemic, countries adopted isolation and quarantine measures for those who traveled to and from the Hubei Province in China and any individuals who were in contact and/or in close quarters with these travelers. These measures were subsequently also adopted for travelers from countries with high COVID-19 infection rates. As individuals arrived by air and sea, the United States opted to implement mandatory quarantines for the purported incubation period of COVID-19. While air travelers have been set up on land at quarantine facilities, sea travelers have been held offshore on cruise ships, unable to disembark. For example, in February and March 2020, several cruise ships were held off the coasts of the United States, Japan, and Hong Kong, establishing mandatory onboard quarantines, holding passengers on the ships, and confining them to their rooms for two weeks.

The CDC (2020b) published guidelines for dealing with individuals exhibiting COVID-19 symptoms. While the CDC recommends medical evaluation for high-risk individuals that are symptomatic, many of the actions proposed by the CDC in its guidelines are largely dependent on the individual and their desire to self-report or self-quarantine. Accordingly, the individual is self-driven to exercise restraint, report symptoms, and remain in isolation and quarantine for the duration of the incubation period. The reality is that individuals might not link their symptoms to COVID-19, report their symptoms, and implement/adhere to voluntary self-isolation or quarantine.

Border Closings and Travel Restrictions

Between January and June of 2020, several regions of the world opted to close their borders and impose travel restrictions on travelers from countries with high COVID-19 infections. As a border security measure, airports implemented exit and entrance screening methods in an effort to identify and isolate those individuals who are exhibiting symptoms consistent with COVID-19 infection. Airport entry and exit screening has included a mixture of traveler self-reporting and examinations by airport and airline staff. Self-reporting consists of passengers answering questions and/or filling out documents or travel cards concerning their travel history, contact history with infected individuals, and whether or not they have any "flu-like" symptoms (fever, cough, and general signs of illness). Screening methods conducted by airline and airport staff include general visual examinations looking for signs of illness and flu-like symptoms such as respiratory distress, coughing, and sneezing, along with the utilization of fever screening methods. Fever screening methods include the utilization of infrared thermometers (also referred to as infrared thermal scanners), which can be placed on the skin or in the ear. A more commonly used noncontact infrared thermometer does not involve human contact; instead, the thermometer is aimed at the passenger's forehead for rapid measurement of body temperature. These devices work by measuring body surface temperature and are different from contact thermometers that measure body core temperature (such as an oral thermometer). Surface temperature readings may not be as accurate as core temperature readings, because surface temperature is subject to acute environmental factors. Consequently, screening

with noncontact infrared detection systems may result in false positive and false negative results.

Several problems exist with border screening methods. First, the standards and methods for vetting passengers at the border, including policies of airlines and airports as well as the individual observational skills of airline employees and designated airport screeners, can vary. Second, the virus itself makes screening challenging since the incubation period makes it possible for infected individuals to travel before exhibiting symptoms and individuals may not exhibit the symptoms screeners look for. Third, the infrared thermometers are measuring surface temperature, so symptoms can be masked with fever medications (antipyretic). In one case, the news reported that a woman in France boasted on social media how she was able to evade airport screening in Wuhan and travel to France by taking fever-reducing medications to mask her "flu-like" symptoms (Mahbubani 2020). Finally, given that these procedures rely on self-reporting, people may not be truthful when answering questions or filling out the forms or they may not know if they were in contact with or in close proximity to an infected person. Even quarantined individuals being monitored present concerns. In January 2020, the news reported that an American attempted to flee a military base while being held for medical clearance after being evacuated from Wuhan, China (Jordan 2020).

Despite the subjectivity in screening methods and the variation in symptoms exhibited by infected individuals, visual screening and self-monitoring remain the two primary methods of preventing the spread of COVID-19. The rapid spread of the virus at the onset and the continued rise in cases into the second half of 2020 demonstrate that such measures may not be the most effective in maintaining national security. The implementation of universal travel and border control guidelines and more objective screening methods at the onset of a suspected outbreak, as well as the establishment of clear and consistent policies and procedures for quarantine and isolation, are needed.

Conclusion

Health security is an essential element of national security. Infectious diseases can destabilize nations due to their high death tolls and staggering economic, psychological, and social consequences. While the United States and other countries have responded to the COVID-19 outbreak with precautionary measures in the form of passenger isolation, travel restrictions, and border screening, these actions were not applied uniformly and therefore were not capable of preventing the spread of the virus domestically. Much is still unknown regarding the epidemiology and health impacts of COVID-19. The implementation of universal travel and border control guidelines and more objective screening methods at the onset of a suspected outbreak, as well as the establishment of clear and consistent policies and procedures for quarantine and isolation, are needed.

Cross-References

- ▶ Border Security
- ▶ Natural Hazards: Pandemic Threats by Infectious Diseases

References

Achenbach, J. (2020). Coronavirus came from bats or possibly pangolins amid 'acceleration' of new zoonotic infections. *The Washington Post*, February 7, 2020. https://www.washingtonpost.com/health/coronavirus-came-from-bats-or-possibly-pangolins-amid-acceleration-of-new-zoonotic-infections/2020/02/07/11eb7f3a-4379-11ea-b503-2b077c436617_story.html

Centers for Disease Control and Prevention (CDC). (2020a). Coronavirus disease 2019 (COVID-19): Overview of testing for SARS-CoV-2. Retreived from https://www.cdc.gov/coronavirus/2019-ncov/hcp/testing-overview.html on May 29, 2020.

Centers for Disease Control and Prevention (CDC). (2020b). Coronavirus Disease 2019 (COVID-19): Public health guidance for potential COVID-19 exposure associated with international travel or cruise travel. Retreived from https://www.cdc.gov/coronavirus/2019-ncov/php/risk-assessment.html on May 29, 2020.

Jordan, M. (2020). Inside the California Military Base a coronavirus evacuee tried to flee. *The New York Times*,

January 30, 2020, https://www.nytimes.com/2020/01/30/us/coronavirus-americans-evacuate.html
Mahbubani, R. (2020). A Chinese embassy in Paris tracked down a woman who gloated on social media about cheating airport detection with a medicine that lowered her fever. *Business Insider*, January 24, 2020, https://www.businessinsider.com/wuhan-coronavirus-woman-avoided-airport-tests-travel-france-2020-1
Maras, M.-H. (2014). *Transnational security.* Boca Raton: CRC Press.
Maras, M.-H., & Miranda, M. D. (2015). State intervention during public health emergencies: Is the United States prepared for an Ebola outbreak? *Journal of Homeland Security and Emergency Management, 12*(2), 257–271.

Further Reading

Maras, M.-H., & Miranda, M. D. (2015). State intervention during public health emergencies: Is the United States prepared for an Ebola outbreak? *Journal of Homeland Security and Emergency Management, 12*(2), 257–271.

Homeland Security Act of 2002

James M. Duggan and James J. F. Forest
Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Keywords
Department of Homeland Security · US Congressional Legislation · Federal Government · Terrorism · Counterterrorism

Definition

An Act passed by the Congress and signed into law by President George W. Bush creating the Department of Homeland Security and reorganizing several other government agencies.

Introduction

The attacks of September 11, 2001, created considerable fear among the US population and pressure for the government to punish those responsible for the attacks, as well as to better secure the homeland. The USA responded with a "war on terrorism" and the largest reorganization of the US government apparatus since the Central Intelligence Agency (CIA) and Department of Defense (DoD) were created in the wake of World War II (Crenshaw and Lafree 2017). President George W. Bush and his staff moved quickly to address the identified weaknesses and vulnerabilities within our counterterrorism structure, while some within the government made pleas for a more judicious approach to such an extensive reorganization (Chang 2014; Crenshaw and Lafree 2017). Nonetheless, the Homeland Security Act of 2002 (*the Act*) was quickly drafted and passed with overwhelming approval, effectively creating the Department of Homeland Security (DHS) and implementing a monumental restructuring of our nation's counterterrorism assets.

The Act and its creation of the DHS were intended to provide "...a single, unified homeland security structure that will improve protection against today's threats and be flexible enough to help meet the unknown threats of the future" (Bush 2002, p. 2). The Act enhanced the role of the Federal Emergency Management Agency (FEMA), making FEMA responsible for leading national emergency preparedness and response efforts, whereas FEMA had previously provided assistance, rather than leadership to state, local, and tribal agencies (Brattberg 2014). The Act tasked FEMA with the creation of a comprehensive response and recovery plan at the national level and served as the primary mechanism to administer an *all hazards* and whole of government approach to our national security efforts (Brattberg 2014). The Act created a comprehensive national security structure, addressing myriad concerns such as border and transportation security, cyber security, chemical, biological, radiological, and nuclear (CBRN) threats, and a unified information and intelligence component to formulate a comprehensive homeland security package (Bush 2002). This entry will briefly review the priority items within the Act and their importance to our homeland security. The Federal Emergency Management Agency, border security, and DHS will be covered in greater detail in other chapters within this volume entitled

► "Federal Emergency Management Agency", ► "Border Security", and ► "Department of Homeland Security (DHS)".

Definitions

Homeland security is officially defined by the *National Strategy for Homeland Security* as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" (US Department of Homeland Security 2007, p. 3). Critical information and key resources (CIKR) are publically or privately controlled resources that are deemed essential to the minimal operations of the economy and government (Congress 2002). Some examples of the 16 critical infrastructure sectors are emergency services, financial services, energy, communications, and dams. Much of our CIKR within the USA are privately owned and managed, requiring collaboration with the private sector in order to assure minimal operations in the case of an emergency. Terrorists are criminals who commit or directly support acts of violence in order to achieve some type of sociopolitical objectives and are covered in more detail in the ► "Criminals: Terrorists" chapter within this volume.

Homeland Security Act of 2002

In the immediate aftermath of the September 11, 2001, terrorist attacks in New York City and Washington, DC, there was a great deal of public fear about the threat of future terrorist attacks and strong pressure for the Congress and the Bush administration to act quickly and decisively to address this threat. There was also no shortage of attempts to blame the attacks, and our perceived vulnerability to terrorism, on a variety of government agencies responsible for border security, transportation security, national security intelligence, and much more. On October 8, 2001, President Bush issued Executive Order 13228 creating an Office of Homeland Security within the White House and a Homeland Security Council, both having specific responsibilities for coordinating efforts against terrorism. However, some members of Congress felt a new federal agency, or full Cabinet-level department was needed in order to more comprehensively address the threat of terrorist attacks against the homeland. Just a few days later, Senators Joe Lieberman and Arlen Specter introduced legislation (Senate Bill 1534) to create a Department of Homeland Security. This legislation was debated for several months through various hearings and committee meetings, but never made it to the Senate floor for a formal vote.

On June 6, 2002, President Bush addressed the nation and proposed the creation of a permanent Cabinet-level Department of Homeland Security. Although the President of the USA may propose legislation, only the Congress can sponsor and pass the legislation necessary to create a new Cabinet-level department. On June 18 the White House submitted to the Congress a formal proposal to establish the DHS, along with proposed text for what became the Homeland Security Act of 2002. On June 24, Rep. Dick Armey sponsored the proposal for introduction to the House of Representatives as H.R. 5005. After amendments in committees, the bill was passed on July 26, 2002, by a vote of 295 to 132. Then the Senate spent several months debating and amending the legislation, which was finally passed by a vote of 90 to 9 on November 19, 2002.

The Act was signed into law by President Bush on November 25, 2002, and presented sweeping changes to our homeland security efforts. The Act established the DHS and merged responsibility for critical issues of homeland security under one umbrella (Brattberg 2014). DHS became responsible for the protection of CIKR, emergency preparedness, and the sharing of information among federal, state, local, and tribal agencies (Brattberg 2014). More specifically, the Act declared the primary mission of DHS to include the following: (1) prevent terrorist attacks within the USA; (2) reduce the vulnerability of the USA to attack; (3) minimize the damage from and assist in the speedy recovery from a successful attack; (4) act as a "focal point" for natural, as well as man-made disasters, and for the emergency planning relative

to those events; (5) identify and disrupt connections between illegal drug trafficking and terrorism; and (6) assure that the efforts of DHS to secure the homeland do not negatively impact the economic security of the USA (Congress 2002).

The Act also transferred 22 existing federal offices into DHS, with the intent of consolidating agencies with a responsibility for homeland security under one umbrella (Brattberg 2014). Among the more noteworthy agency offices that were transferred into DHS were the US Customs Service, the Federal Protective Service (which provides police services at federal buildings), the Transportation Security Administration (TSA), the Federal Law Enforcement Training Center, the Federal Emergency Management Agency (FEMA), the US Secret Service, and the US Coast Guard (Crenshaw and LaFree 2017).

Because the threat was viewed as originating from outside the USA, border security was afforded considerable attention (Crenshaw and LaFree 2017). The Act established the Directorate of Border and Transportation Security, which assumed control of several transferred departments and agencies. The Immigration and Naturalization Service (INS) and the US Customs Service were transferred under the control of the Directorate of Border and Transportation Security, with INS to be abolished upon completion of record transfers (Congress 2002). The Directorate of Border and Transportation Security divided the duties of INS and US Customs between three new departments: the Bureau of Customs and Border Protection, the Bureau of Citizenship and Immigration Services, and the Bureau of Immigration and Customs Enforcement (ICE) (Congress 2002). In turn, ICE absorbed the Federal Protective Service (FPS) and US Customs Service to form the largest investigative agency within DHS (Crenshaw 2017). ICE was entrusted with the duty to protect the country's borders from penetration by terrorist actors, as well as weapons and weapon components (Crenshaw 2017). In addition, the Act established a program that would allow volunteer pilots to be armed and deputized as federal law enforcement officers (Congress 2002).

The Act also established a Directorate for Information and Analysis (I&A) within DHS that was charged with the duty of providing information and intelligence in support of DHS (Brattberg 2014). DHS I&A was expected to accomplish this mission by collaborating with state and local agencies, as well as the private sector, to identify and assess terrorist threats to the homeland within the context of vulnerabilities previously identified by I&A (Congress 2002). In addition, I&A was required to develop a national plan to protect our CIKR by first conducting vulnerability assessments followed by the creation of a plan to protect not only the physical assets of our CIKR but also the technologies required to support the resiliency of those resources (Congress 2002). The Act also entrusted DHS I&A with the daunting task of developing policies for improving the sharing of information and intelligence among federal agencies, as well as between the federal, state, local, and tribal agencies (Congress 2002). DHS was later relieved of this task with the creation of the Office of the Director of National Intelligence on 2004.

With the implementation of the Act, FEMA took the lead in training, planning, and coordinating with state and local agencies to prepare for the response and recovery from man-made (terrorist) as well as natural disasters (Bush 2002). Prior to implementation of the Act, the federal government had primarily assisted state and local agencies by augmenting their equipment and personnel resources in the case of a large-scale natural disaster (Brattberg 2014). DHS' new planning and response capabilities included the ability and responsibility to detect and counter chemical, biological, radiological, and nuclear (CBRN) threats. In addition, DHS was tasked with developing a national interagency response and communication plan, which would lead to the development of the National Incident Management System (NIMS). The Department of Health and Human Services (HHS) was also transferred to DHS, despite warnings against the transfer because of lack of congruency between the missions of the two agencies (Rittgers 2014). DHS therefore assumed the HHS responsibility

for maintaining a stockpile of pharmaceutical drugs that would be necessary in the case of assorted disasters and assumed the obligation of managing grant funding to assist state and local first responders (Congress 2002).

Conclusion

The creation of the DHS has been criticized by some for being too rushed, a hasty reaction to a politically charged environment in which the threat of terrorism may have been exaggerated. Of course, even with meticulous planning, such a massive restructuring of government agencies could be expected to be rife with pitfalls, but the expeditious implementation of the Act and launching of DHS all but assured those pitfalls (Rittgers 2014). Virtually no American citizen has been unaffected by the sweeping changes in security policies that have emerged in the years following the passage of the Homeland Security Act of 2002. But despite criticisms, the survival of the DHS was recently assured with the DHS Authorization Act of 2017, which committed the USA to improving the weaknesses within DHS by consolidating programs, controlling spending, and providing greater support to state and local first responders, rather than initiating a superseding reorganization of our homeland security agencies (Congress 2017).

Cross-References

- ▶ Border Security
- ▶ Department of Homeland Security (DHS)
- ▶ Federal Emergency Management Agency
- ▶ Investigations: Terrorism

References

Brattberg, E. (2014). Coordinating for contingencies: Taking stock of post-9/11 homeland security reforms. In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism: Readings and interpretations* (2nd ed.). New York: McGraw-Hill.

Bush, G. W. (2002). *The department of homeland security.* Washington, DC: White House.

Chang, N. (2014). The USA Patriot Act: What's so patriotic about trampling on the bill of rights? In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism: Readings and interpretations* (2nd ed.). New York: McGraw-Hill.

Crenshaw, M., & Lafree, G. (2017). *Countering terrorism*. Washington, DC: Brookings Institution Press.

Congress (2002). Pub. Law 107-296. *The Homeland Security Act of 2002*. Washington, DC: Congress.

Congress (2017). H.R. 2825. *Department of Homeland Security Authorization Act of 2017*. Washington DC: Congress.

Rittgers, D. (2014). Abolish the department of homeland security. In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism: Readings and interpretations* (2nd ed.). New York: McGraw-Hill.

The U.S. Department of Homeland Security. *National Strategy for Homeland Security,* October 2007. Online at: https://www.dhs.gov/national-strategy-homeland-security-october-2007.

Further Reading

Bush, G. W. (2002). *The department of homeland security.* Washington, DC: White House.

Forest, J. (2018). *The terrorism lectures* (3rd ed.). Santa Ana: Nortia Press.

Congress. (2017). H.R. 2025. *Department of Homeland Security Authorization Act of 2017*. Washington, DC: Congress.

Public Law 107-296. (2002). *The Homeland Security Act of 2002*. Washington, DC: Congress.

The U.S. Department of Homeland Security, History Office. Brief Documentary History of the Department of Homeland Security, 2001–2008. Online at: https://www.hsdl.org/?view&did=37027

Human-Made Disasters: Electric Power and Transit Linked Outages

Rae Zimmerman
Institute for Civil Infrastructure Systems, Robert F. Wagner Graduate School of Public Service, New York University, New York, NY, USA

Keywords

Electric power · Rail transit · Infrastructure interdependencies · Power outages · Natural hazards · Human unintentional and intentional actions

Definition

Electric power outages related to transit service continuity are associated with a number of factors that originate in transit and electric power system characteristics, such as the capacity to withstand equipment issues; environmental conditions, including natural hazards, such as extreme weather and climate change impacts on energy systems (U.S. DOE 2013a) and human responses to those conditions; unintentional human actions, such as the accidental, inadvertent disruption of a power line or street salting; and intentional human acts, such as sabotage and cyberattacks (Zimmerman 2012a, Chapter 7; Zimmerman 2017).

Introduction

The scope of electric power and transit linkages in this entry signifies connections between electric power and rail transit systems primarily to move transit vehicles that provide vital transportation services. Electric power is also used for supporting facilities such as signals, switches, lighting for rail, vehicles, and stations and for cleaning and servicing equipment; however, the electric power linkages to these functions are not within the scope of this entry. There are many different forms of transit, and this entry focuses on public rail transit as distinct from buses and paratransit. Within the category of rail transit, the focus is on heavy rail, since in the USA according to the National Transit Database (NTD) (US Department of Transportation (DOT), Federal Transit Administration (FTA), NTD, 2018a), heavy rail accounts for a large part of the services and activity relative to all transit systems. According to calculations from the NTD, heavy rail accounts for among the highest levels of passenger travel in terms of trips, which is a little over a third of passenger trips, and about a third of all passenger miles traveled (U.S. DOT, FTA, NTD 2018a). Heavy rail passenger trips also were reported by U.S. DOT, FTA, NTD, Office of Budget and Policy (2019a: 21) to have increased by 6.7% from 2009 to 2018. Heavy rail accounted for half of all rail security incidents in the period from 2009 to 2018, and two-thirds of those were related to security, most occurring at train stations (U.S. DOT, FTA, NTD, Office of Budget and Policy 2019b, p. 21). Heavy rail ranks high in annual energy use among other transit systems (U.S. DOT, FTA, NTD 2018b, Fuel and energy_2.xlsm).

Electric power is important for transit performance since energy is one of transit's essential resources. The transition of rail systems to electric power occurred over a period of a few decades following the introduction of rail transit. The extent of rail transit energy usage and electric power outages and the impact of such outages on transit are key aspects of the viability of public transportation. This entry covers these issues for heavy rail transit.

Heavy Rail Transit in the USA

Heavy rail is defined by the National Transit Database (NTD) (U.S. DOT, FTA, NTD, Glossary 2020, pp. 32–33): "A transit mode that is an electric railway with the capacity for a heavy volume of traffic. It is characterized by: – High speed and rapid acceleration passenger rail cars operating singly or in multi-car trains on fixed rails – Separate rights-of-way (ROW) from which all other vehicular and foot traffic are excluded – Sophisticated signaling – High raised platform loading."

The US Department of Transportation (DOT) Federal Transit Administration (FTA) NTD (2018a) lists 15 heavy rail transit systems in the USA. Together, these systems accounted for 3,724,442,285 unlinked passenger trips in 2018 exceeded by bus transit which was close to 4 billion trips (U.S. DOT, FTA, NTD 2018a, NTD data, 2018 Metrics). The largest of these systems is the Metropolitan Transportation Authority (MTA) New York City Transit system which in 2018 served a US Bureau of the Census-defined urbanized area (U.S. DOT, FTA, NTD 2020, Glossary) of over 18 million people; accounted

for 2.7 billion annual unlinked passenger trips which is about ten times the passenger trips for the second and third largest heavy rail systems; and accounted for about 70% of US heavy rail unlinked passenger trips and about 60% of passenger miles (calculations from the U.S. DOT, FTA, NTD 2018a, NTD data, 2018 Metrics). Given its size, the NYS MTA will be emphasized in the presentation of electric power and transit linkages.

The reliance of heavy rail on electric power is underscored by the NTD (U.S. DOT, FTA, NTD 2019b, p. 3):

"Heavy Rail (HR) is an electric railway that operates service in an exclusive right-of-way." (U.S. DOT, FTA, NTD, Office of Budget and Policy 2019b, p. 3). The NTD indicates that other transit systems run on electric power as well, but heavy rail seems to consume more electric power (U.S. DOT, FTA, NTD (2018b) 2017 Fuel and Energy_2.xlms). Electric power consumption is reported by the NTD as "electric propulsion" defined as "kilowatt-hours of electricity used to propel vehicles directly providing power to a third rail or overhead catenary" (U.S. DOT, FTA, NTD (2018b) 2017 Fuel and Energy_2.xlsm Data Dictionary). In 2017, the electric propulsion for the 15 heavy rail transit systems in the USA totaled 3,728,009,564 kWh (U.S. DOT, FTA, NTD (2018b) 2017 Fuel and Energy_2.xlsm), or 56% of the total electric propulsion reported for all transit systems totaling 6,604,153,364 kWh (not only rail transit). NYC Transit consumed 1,624,428,000 kWh in terms of electric propulsion, which was a quarter of the 6,604,153,364 kWh for all US transit systems and 44% of the 15 heavy rail transit system consumption of electric propulsion of 3,728,009,564 kWh (U.S. DOT, FTA, NTD 2018b, 2017 Fuel and Energy_2.xlsm).

The History of Rail Transit and Its Energy Sources

The connection between electric power and rail transit increased over time following the introduction of the first rail transit systems. The first rail transit systems were the London Underground subway in 1863 transporting 40,000 people in the first day of operation and the Boston, MA, subway which opened in 1897 consisting of 3 stations under 1 mile in length (HERE Mobility 2019, p. 11 citing Coldwell 2013 for London and Brooks 2017 for Boston). In the nineteenth century, rail travel relied on wood for power, then coal to produce steam, and diesel. As described by Lothes (2009), the electrification of the first rail system is said to date back to 1895; by 1939 the USA accounted for a fifth of the world total.

In addition to heavy rail transit systems reported by the NTD, other heavy rail systems have substantial reliance on electric power. Amtrak's use of electric power for train energy consumption generally was reported as increasing from 1975 to 2008 (180 million kWh to 582 million kWh), decreasing thereafter through 2015 to 504 million kWh, and increasing to 516 million kWh in 2016 (U.S. DOT, Bureau of Transportation Statistics, 2019, Table 4–18). Amtrak (2018, p. 12) indicates that electricity ranks second to diesel fuel for energy consumption and estimates that about three quarters of the electricity is used for trains with the rest for other uses.

New York City subways were converted to electric power at the turn of the twentieth century, with the banning of steam-driven commuter railroads by 1908 south of the Harlem River, and the transition was attributed to an accident on January 8, 1902, involving steam-powered trains that obscured signals (Horn 2015; NYSDOT undated; Lothes 2009). In the New York area rail transit system, the New York Metropolitan Transportation Authority (MTA) exemplifies how the relationship of one of its components, the subway system (New York City Transit), changed over time in terms of its electric power providers. NYC once had its own electric power substations, 75 of them, most of which were built in the early twentieth century (Payne 2002, p. 31). They received electric power from power stations, converting the power from alternating current (AC) to direct current (DC), lowering voltage for distribution of power to the third rail, and

considered one of the last such "manually operated" systems (Payne 2002, p. 12). In 1959, Con Edison bought several of the MTA power plants in return for Con Edison agreeing to provide the subway system with electric power (Payne 2002, p. 53).

The NYC subway transitioned initially from steam to electricity and then to diesel with electricity continuing to dominate the power sources. In the late nineteenth century when the first rapid transit systems emerged in NYC, they relied upon steam-powered locomotives (Payne 2002, p. 15). Electrification of rail is attributed first to have occurred for overhead electrical lines in Richmond, VA, in 1888, followed by the electrification of Chicago's third rail in 1895, with New York City following with electrification of its elevated train lines from 1898 to 1903 (Payne 2002, p. 15). In the twenty-first century, newer sources of electricity emerged such as solar energy described later, applied to rail transit, primarily as a power source for stations. Diesel locomotives continue to be used for emergency purposes, for example, by the NYS MTA, either to move stalled trains or to provide limited service on disabled lines, and were used, in September–October 2013 for the New Haven Line power failure (Flegenheimer 2013). Diesel-powered generators are increasingly relied upon for emergencies with new generators purchased, for example, for the MTA LIRR (MTA 2019a, p. 39).

Electric power is distributed to the NYC subway system by Con Edison; power sources include the New York Power Authority (MTA Undated (a), pp. 5, 13) and others (Con Edison 2019a, b). Electric power sources for the NYC subway system vary depending upon the system component. The third rail runs on one type of power, and the signals and lighting run on another source. The MTA reports that by type of power "Alternating current (AC) operates signals, station and tunnel lighting, ventilation, and miscellaneous line equipment and Direct current (DC) operates trains and auxiliary equipment, such as water pumps and emergency lighting." "Substations receive as much as 27,000 volts from power plants and convert it for use in the subway. The third (contact) rail uses 625 volts to operate trains" (MTA undated (b), p. 4).

Impacts of Electric Power Outages for Transit

Electric power outages in the USA have generally increased in terms of frequency and duration (Simonoff et al. 2007), which are the common measures of electricity performance. With respect to system reliability, the NYS Department of Public Service (DPS) (2019, p. 1 and footnote 1) has adopted these two measures typically used in the industry for frequency and duration of outages: "the System Average Interruption Frequency Index (SAIFI or frequency) and the Customer Average Interruption Duration Index (CAIDI or duration)" defined in the following way: "SAIFI is the average number of times that a customer is interrupted for five minutes or more during a year. CAIDI is the average interruption duration time in hours for those customers that experience an interruption during the year." These measures and similar ones are applied to urban areas (Blake et al. 2019; National Academies of Sciences, Engineering and Medicine 2016a). Electric power outages are generally related to a number of factors associated with system characteristics and environmental conditions that vary for underground and overhead electric power lines. As indicated above in the definition, these factors include natural hazards such as extreme weather and climate change (U.S. DOE 2013a); equipment malfunctions; unintentional human actions such as the accidental, inadvertent disruption of a power line or street salting; and intentional human acts such as sabotage and cyberattacks (Zimmerman 2012a, Chapter 7; Zimmerman 2017).

Electric power outages are a source of transit outages though not the only source of such outages as indicated above. Heavy rail transit systems are typically connected to electric power grids and as such are vulnerable to outages that affect the power. In addition, when power is restored, it can take additional time for the transit systems to be

restored (Zimmerman and Restrepo 2006) given the multiplier effect created by the need for adjustments and inspections before the systems are put back in service. After Hurricane Sandy, heavy rail train service was not fully restored for a week or more after the storm; The NYC subway system and other heavy rail lines such as the PATH had pumped out much of the water but had to await power restoration to restart the system (NYS 2100 Commission 2013, p. 45; Kaufman et al. 2012; Zimmerman 2014; Zimmerman 2016). Major hurricanes have resulted in extensive power outages that often have long restoration times (Miles et al. 2014, 2015; U.S. Department of Energy 2013a, p. 2; 2013b), and these cases have been recognized in research on infrastructure interdependencies (Zimmerman et al. 2017; Zimmerman 2020 forthcoming). Many of these power outages have been associated with transit outages. Although extreme weather is a natural hazard, the extent of the consequences is often affected by human activity (National Academy of Sciences 2016b).

Transit has been shown to be vulnerable to power outages in large outages that are not weather-related, and as in the case of weather-related outages, the effects can be magnified by the duration of recovery. Zimmerman and Restrepo (2006, p. 223) reported that after the 2003 US-Canada blackout, for example, NYC transit systems took 1.3 times longer to be restored than the time it took for the power itself to be restored. A massive electric power outage in London on August 9, 2019, created extensive transit delays before service was restored, and though it took under an hour for power restoration, transit services were not restored until the next day (Karasz 2019). In Buenos Aires and neighboring parts of Uruguay, a power outage in June 2019 specifically disabled the transit system (Trevisani and Lewis 2019). A massive disruption created by the disabling of 135,000 kV power lines for the MTA Metro-North system lasted weeks after the voltage problem was restored at least temporarily (Flegenheimer 2013; MTA 2014).

For New York City, the NYS Governor has attributed numerous delays in subway service to power (French and Rubinstein November 21, 2017, Paragraph 2). In April 2017 the system experienced damage to a 53rd Street and 7th Avenue energy system resulting in cascading failures of numerous subway lines (French and Rubinstein 2017). Power failures occurred again on May 7, 2019, and in July 2019, some of which affected transit.

Unintentional acts that lead to power outages include equipment disruptions, for example, from 2016 and 2019, a number of high-profile outages were accompanied by transit stoppages in New York City. Intentional acts such as terrorism have disrupted heavy rail systems either directly, or service has been disrupted indirectly by preemptive shutdowns in anticipation of such events. Both of these situations occurred in NYC after the World Trade Center attacks of September 11, 2001.

In New York State, extreme weather events were separated from non-weather-related phenomena in connection with electric power outages. The NYS Department of Public Service (2019, p. 7) concluded that excluding storms, most of the outages were attributed to "equipment failure and tree contact." From March through May of 2018, the department identified five major storms that add to a total of 1.136 million outages (some statewide, some regional), and the duration of the outages sometimes exceeded 3 days (NYS Department of Public Service 2019, pp. 9–10).

Innovations to Improve Resilience for Both Electric Power and Transit

Innovations in the use of electric power are emerging that have the potential to reduce electric power impacts for rail and promote sustainability (Abdallah 2017, pp. 61–65). Many of these are technological. Regenerative braking is one way to conserve electric power by enabling the train system to use its own power. The NYS MTA (MTA Undated (a), p. 13) describes the use of regenerative braking in its "New Technologies subway cars (also called New Millennium Trains)"

models R-142, R-142A, R-143, and R-160 on selected subway lines where energy normally lost as heat is returned to the third rail through regenerative braking. Some of the conditions of using this technology are the timing of the generation and its transfer to another train (González-Gil et al. 2013). Storage systems have been explored in some heavy rail transit systems to enable such transfers to occur (Chicago Transit Authority (CTA) and Mott MacDonald 2017).

Other options are changing the material used for the third rail to reduce the amount of energy lost, for example, "Since aluminum is a better conductor of electricity than steel, NYC Transit is experimenting with two kinds of aluminum third rails to save energy: an all-aluminum rail with a stainless steel cap on its contact surface; and a steel-and-aluminum hybrid rail that has a steel base and aluminum cladding on its sides. Aluminum is also lighter than steel, which means aluminum-component rails are easier to handle, install, and replace than conventional steel rails" (MTA Undated (a), p. 13).

Another technology is called the "Subway Car Shunting Elimination Program" that began in 1996, considered "one of its most successful energy conservation projects. By modulating the acceleration rate and limiting the top speed of the 5,800-car subway fleet, NYC Transit reduces energy use per subway car mile by 12 percent and saves 240 million-kilowatt hours of electricity annually" (MTA Undated (a), p. 13).

Increased use of renewable energy is an option but also relies upon storage. The Coney Island Stillwell station is an important example of the use of solar energy for station lighting and other support systems. Other rail transit systems are similarly tapping solar energy, for example, Boston's T line uses solar energy primarily for support facilities such as parking, rail yards, and garages (Massachusetts Bay Transportation Authority (MBTA) undated). It is not certain what the extent of solar power usage is to power trains directly unless it is used indirectly by sources tapped for electric power in general. Energy storage systems, wayside energy storage system (WESS), are being considered for transit systems to save on energy use through voltage stabilization (Abdallah 2017). Chicago is an illustration of the introduction of this technology into transit (Chicago Transit Authority and Mott MacDonald 2017).

Energy conservation in general is potentially a way to protect against the vulnerability of electric power outages. Energy intensity reflects energy conservation, measured in terms of Btu per passenger mile, and varied in 2016 for US heavy rail systems from about 500 to 3250 Btu per passenger mile; New York ranked second lowest with a little over 500 Btu per passenger mile (Davis and Boundy 2019, p. 2–22).

Other options for potentially promoting resilience in electric power systems for transit relate to electric power alone (Con Edison et al. 2013; Con Edison 2017a) and for transit alone (MTA 2016; MTA 2019b) which tend to be operational. For example, with respect to NYC Transit, on August 2, 2017, Con Edison (2017b) issued a statement indicating its approach to reducing the impact of power outages on the subway system in response to the NYS Public Service Commission (Con Edison 2017b, Paragraph 2).

Resiliency options involving transit alone have been addressed separately by the MTA in connection with extreme events and climate change (Jacob et al. 2008; Zimmerman 2012b; Jacobs et al. 2018; MTA 2019b; Zimmerman et al. 2019).

Observations and Conclusions

Electric power outages pose a key vulnerability to public transit and particularly to heavy rail transit, which is the focus of this inquiry. Power-related transit conditions are reflected in the apparent increase in the number of power outages and the effect on transit. This is a significant problem given the substantial ridership these systems account for and the need to reduce vulnerability to those populations and promote resiliency and sustainability that transit systems offer. As newer technologies emerge and may potentially be applied to rail transit, such as autonomous vehicles, the impact upon electric power usage will need to be evaluated along with the implications of power outages to those technologies.

Ways of reducing this vulnerability are emerging and are potential solutions for electric power and transit. Making progress toward this goal will require attention on the part of both of these systems simultaneously and the recognition of the dependency of transit on electric power to move toward solutions. Electric power and transit will have to come together in terms of technology, social, and environmental impacts, and the institutions overseeing them will play a major part in the integration of these two systems.

Cross-References

- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Emergency Management: Crisis Management and Response
- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
- ▶ Natural Hazards: Hurricanes, Cyclones, and Typhoons
- ▶ Physical Security: Best Practices

Acknowledgments This work was supported by the following grants or cooperative agreements listed below:
The National Science Foundation under Cooperative Agreement #1444755, the Urban Resilience to Extremes Sustainability Research Network (UREx SRN).
"Critical Resilient Interdependent Infrastructure Systems and Processes (CRISP) Type 1: Reductionist and integrative approaches to improve the resiliency of multi-scale interdependent critical infrastructure," funded by the NSF (#1541164).
"Dynamic Resiliency Modeling and Planning for Interdependent Critical Infrastructures," funded by Critical Infrastructure Resilience Institute (CIRI), U. of Illinois, Urbana-Champaign, supported by the US Department of Homeland Security under Grant Award #2015-ST-061-CIRC01.
"Developing Secure Strategies for Vehicular Ad hoc Networks in Connected and Autonomous Vehicles," from C2SMART, NYU Tandon School of Engineering, US Department of Transportation. US DOT award number 69A3551747124.
Disclaimer: Any opinions, findings, views, conclusions, or recommendations expressed in this material are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the National Science Foundation, the US Department of Homeland Security, or the US Department of Transportation.

References

Abdallah, T. (2017). *Sustainable mass transit. Challenges and opportunities in urban public transportation*. Amsterdam: Elsevier.

Amtrak. (2018). Amtrak Sustainability Report 2016–2017. Retrieved from https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/environmental1/2016-2017-Amtrak-Sustainability-Report.pdf

Blake, R., Jacob, K., Yohe, G., Zimmerman, R., Manley, D., Solecki, W., & Rosenzweig, C. (2019). New York City Panel on Climate Change 2019 Report Chapter 8: Indicators and Monitoring. In: C. Rosenzweig, W. Solecki (Eds.), *Advancing Tools and Methods for Flexible Adaptation Pathways and Science Policy Integration: NPCC 2019 Report*. Special Issue: Annals of the New York Academy of Sciences. 1439, pp. 230–279. https://doi.org/10.1111/nyas.14014

Brooks, R. B. (2017). History of the Boston subway: The first subway in America History of Massachusetts (blog). Retrieved from https://historyofmassachusetts.org/boston-first-subway-america/

Chicago Transit Authority (CTA), & Mott MacDonald. (2017). CTA WESS Summary Report A study on how implementing a Wayside Energy Storage System will impact the CTA Red Line. Retrieved from https://www.transitchicago.com/assets/1/28/CTA_Red_Line_WESS_Study_Summary_Report.pdf

Coldwell, W. (2013). 150 facts for 150 years of the London tube. *The Independent*. Retrieved from www.independent.co.uk/life-style/history/150-facts-for-150-years-of-thelondon-tube-8444153.html

Con Edison. (2017a). Our storm-hardening protection plan. Accessed 2 Feb 2019. https://www.coned.com/en/our-energy-future/our-energy-projects/storm-hardening-enhancement-plan

Con Edison. (2017b). Statement from Con Edison Re: PSC Order on MTA Plan. Retrieved from https://www.coned.com/en/about-us/media-center/news/20170802/statement-from-con-edison-re-psc-order-mta-plan

Con Edison. (2019a). How we source our electric power. Retrieved from https://www.coned.com/en/our-energy-future/how-we-source-our-energy/electricity

Con Edison. (2019b). Company history and statistical information. Retrieved from https://www.coned.com/en/about-us/corporate-facts

Consolidated Edison Co. of New York and Orange and Rockland Utilities. (2013). Post-Sandy Enhancement Plan. Retrieved from https://www.coned.com/-/media/files/coned/documents/services-outages/post_sandy_enhancement_plan.pdf.

Davis, S.C., & Boundy, R.G. (2019). *Transportation energy data book* edition 37. Oak Ridge: Oak Ridge National Laboratory. Retrieved from https://tedb.ornl.gov/wp-content/uploads/2019/03/TEDB_37-2.pdf

Flegenheimer, M. (2013). Power failure disrupts Metro North's New Haven Line; May last days. *New York Times*. Retrieved from http://www.nytimes.com/2013/

09/26/nyregion/metro-norths-new- haven-line-suspended-after-power-loss.html

French, M.J. & Rubinstein, D. (2017). Con Ed takes over work, contracts and costs on MTA electrical repairs. *Politico*. Retrieved from https://www.politico.com/states/new-york/albany/story/2017/11/21/con-ed-takes-over-work-contracts-and-costs-on-mta-electrical-repairs-118775

González-Gil, G., Palacin, R., & Batty, P. (2013). Review sustainable urban rail systems: Strategies and technologies for optimal management of regenerative braking energy. *Energ Conv Manage 75*, 374–388. Retrieved from https://doi.org/10.1016/j.enconman.2013.06.039.

HERE Mobility. (2019). The State of Mobility 2019.

Horn, C. (2015). 1902 Park avenue tunnel collision —a new Rochelle tragedy—a work in progress! Retrieved from https://sites.rootsweb.com/~nywestch/NewRoc1902/

Jacob, K., Rosenzweig, C., Horton, R., Major, D. & Gornitz, V. (2008). MTA adaptations to climate change a categorical imperative. MTA. Retrieved from https://new.mta.info/document/10451

Jacobs, J. M., Culp, M., Cattaneo, L., et al. (2018). Transportation. In D. R. Reidmiller, C. W. Avery, D. R. Easterling, et al. (Eds.), *Impacts, risks, and adaptation in the United States: Fourth national climate assessment* (Vol. II, pp. 479–511). Washington, DC: U.S. Global Change Research Program.

Karasz, P. (2019). U.K. seeks answers after biggest power failure in a decade. *The New York Times*. Retrieved from https://www.nytimes.com/2019/08/10/world/europe/uk-power-cut.html?searchResultPosition=3

Kaufman, S., Qing, C., Levenson, N., & Hanson, M. (2012). Transportation during and after Hurricane Sandy. New York, NY: New York University Wagner Rudin Center for Transportation. Retrieved from http://wagner.nyu.edu/files/rudincenter/sandytransportation.pdf

Lothes, S. (2009). The stages of U.S. railroad electrification a brief look at the eras in American railroad electrification. *Trains*. Retrieved from http://trn.trains.com/railroads/railroad-history/2009/09/the-stages-of-us-railroad-electrification

Massachusetts Bay Transportation Authority (MBTA). (Undated). Energy conservation. Retrieved from https://www.mbta.com/sustainability/energy-conservation

Miles, S., Gallagher, H., & Huxford, C. (2014). Restoration and impacts from the September 8, 2011, San Diego power outage. *Journal of Infrastructure Systems, 20*(2), 05014002. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000176.

Miles, S., Jagielo, N., & Gallagher, H. (2015). Hurricane Isaac power outage impacts and restoration. *Journal of Infrastructure Systems, 22*(1).

MTA. (2014). Press release. Metro north. New Haven line power upgrade continues new transformer installed at Mount Vernon substation. Retrieved from http://www.mta.info/press-release/metro-north/new-haven-line-power-upgrade-continues

MTA. (2016). MTA climate adaptation task force resiliency report. Retrieved from https://new.mta.info/document/10456

MTA. (2019a). Annual report to the Governor. Retrieved from http://web.mta.info/mta/compliance/pdf/2018_annual/Annual_Report_Narrative_Updated.pdf

MTA. (2019b). Adaptation task force resiliency report update on agency-wide climate resiliency projects. Retrieved from https://new.mta.info/document/10461

MTA. (Undated-a). MTA Facts and figures. New York City Transit and the environment. Retrieved from http://web.mta.info/nyct/facts/ffenvironment.htm

MTA. (Undated-b). MTA Facts and figures. Subways. Retrieved from http://web.mta.info/nyct/facts/ffsubway.htm

National Academies of Sciences, Engineering, and Medicine. (2016a). *Pathways to urban sustainability: challenges and opportunities for the United States*. Washington, DC: The National Academies Press. Retrieved from https://doi.org/10.17226/23551.

National Academies of Sciences, Engineering, and Medicine. (2016b). *Attribution of extreme weather events in the context of climate change*. Washington, DC: The National Academies Press. Retrieved from https://doi.org/10.17226/21852.

New York State (NYS) 2100 Commission. (2013). Recommendations to improve the strength and resilience of the Empire State's infrastructure. Retrieved from https://www.governor.ny.gov/sites/governor.ny.gov/files/archive/assets/documents/NYS2100.pdf

New York State Department of Public Service (DPS). (2019). 2018 Electric Power Reliability Report. Retrieved from http://www3.dps.ny.gov/W/PSCWeb.nsf/96f0fec0b45a3c6485257688006a701a/d82a200687d96d3985257687006f39ca/$FILE/Electric%20Reliability%202018%20DMM.pdf

NYS Department of Transportation (DOT). (Undated). Passenger Rail Service in NYS. Retrieved from https://www.dot.ny.gov/divisions/operating/opdm/passenger-rail/passenger-rail-service/history-railroads

Payne, C. (2002). *New York's forgotten substations. The power behind the subway*. New York: Princeton Architectural Press.

Simonoff, J. S., Restrepo, C. E., & Zimmerman, R. (2007). Risk management and risk analysis-based decision tools for attacks on electric power. *Risk Analysis, 27*(3), 547–570.

Trevisani, P. & Lewis, J.T. (2019). Argentina, Uruguay blacked out by massive power failure trains halted and traffic signals stopped as nations of more than 57 million people try to cope without electricity. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/argentina-uruguay-blacked-out-by-massive-power-failure-11560696223?mod=searchresults&page=1&pos=1

U.S. Department of Energy. (2013a). *US Energy sector vulnerabilities to climate change and extreme weather*. Washington, DC: U.S. DOE. Retrieved from https://

www.energy.gov/sites/prod/files/2013/07/f2/20130716-Energy%20Sector%20Vulnerabilities%20Report.pdf
U.S. DOE. (2013b). *Comparing the impacts of Northeast Hurricanes on energy infrastructure*. Retrieved from http://energy.gov/sites/prod/files/2013/04/f0/Northeast%20Storm%20Comparison_FINAL_041513c.pdf.
U.S. Department of transportation (DOT) Bureau of Transportation Statistics. (2019). National Transportation Statistics 2018. Retrieved from https://www.bts.gov/sites/bts.dot.gov/files/docs/browse-statistical-products-and-data/national-transportation-statistics/223001/ntsentire2018q4.pdf
U.S. Department of Transportation, Federal Transit Administration. (2020). National Transit Database (NTD) Glossary. Retrieved from https://www.transit.dot.gov/ntd/national-transit-database-ntd-glossary
U.S. Department of Transportation, Federal Transit Administration, National Transit Database NTD. (2018a). Annual Data Tables (agency information, service data, 2018 data product year). 2018 Metrics. Retrieved from https://www.transit.dot.gov/ntd/ntd-data
U.S. Department of Transportation, Federal Transit Administration, National Transit Database. (2018b). Fuel and energy.xlsm. Retrieved from https://www.transit.dot.gov/ntd/data-product/2018-fuel-and-energy
U.S. Department of Transportation, Federal Transit Administration, National Transit Database, Office of Budget and Policy. (2019a). 2018 National Transit Summaries and Trends: Appendix. Retrieved from https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ntd/data-product/134406/2018-ntst-appendix_0.pdf
U.S. Department of Transportation, Federal Transit Administration, National Transit Database, Office of Budget and Policy. (2019b). 2018 National Transit Summary and Trends. Retrieved from https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ntd/data-product/134401/2018-ntst_1.pdf
Zimmerman, R. (2012a). *Transport, the Environment and Security. Making the Connection*. Cheltenham, UK and Northampton, MA: Edward Elgar Publishing, Ltd. ISBN 978 1 84980 020 4.
Zimmerman, R. (2012b). Critical infrastructure and interdependency revisited, chapter 20. In D. G. Kamien (Ed.), *The McGraw-Hill Homeland Security Handbook* (Vol. 2012, 2nd ed., pp. 437–460). New York: The McGraw-Hill Companies, Inc.
Zimmerman, R. (2014). Planning restoration of vital infrastructure services following hurricane sandy: Lessons learned for energy and transportation. *Journal of Extreme Events, 1*(2). https://doi.org/10.1142/S2345737614500043. Retrieved from http://www.worldscientific.com/DOI/pdf/10.1142/S2345737614500043.
Zimmerman, R. (2016). Resilient urban infrastructure for adapting to extreme environmental disruptions, Chapter 32 in The Routledge Handbook of Urbanization and Global Environmental Change. K. C. Seto, W. D. Solecki & C. A. Griffith, (Eds.). New York, NY: Routledge, pp. 488–512. ISBN: 978-0-415-73226-0
Zimmerman, R. (2017). The cyber and critical infrastructures nexus: Interdependencies, dependencies and their impacts on public services. White Paper, NYU Center for Cybersecurity. Retrieved from http://cyber.nyu.edu/wp-content/uploads/2017/12/Zimmerman-122717updateEdited-White-Paper-Cyber-and-Critical-Infrastructures.pdf
Zimmerman, R. (2020forthcoming). Historical and Anticipated Changes in Interconnected and Concentrated Infrastructure and Social Networks in Weather, Climate and Human-Initiated Disruptions, in *Urban Infrastructure: Interdisciplinary Perspectives from History and the Social Sciences*, edited by J. Soffer, J. Heathcott, and R. Zimmerman. Pittsburgh: University of Pittsburgh Press.
Zimmerman, R., & Restrepo, C. E. (2006). The next step: Quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures, 2*(2/3), 215–230.
Zimmerman, R., Zhu, Q., de Leon, F., & Guo, Z. (2017). Conceptual modeling framework to integrate resilient and interdependent infrastructure in extreme weather. *Journal of Infrastructure Systems*. 23(4) (online) 04017034–1 to 13. http://ascelibrary.org/doi/pdf/10.1061/(ASCE)IS.1943-555X.0000394.
Zimmerman, R., Foster, S., González, J. E., Jacob, K., Kunreuther, H., Petkova, E. P., & Tollerson, E. (2019). New York City panel on climate change 2019 report, "chapter 7: Resilience strategies for critical infrastructures and their interdependencies," in New York City panel on climate change (NPCC), advancing tools and methods for flexible adaptation pathways and science policy integration: NPCC 2019 Report. C. Rosenzweig & W. Solecki, (Eds.), Annals of the New York Academy of Sciences, 1439, pp. 174–229. https://doi.org/10.1111/nyas.14010

Human-Made Disasters: Toxic Waste and Residences

Ashley K. Farmer
Illinois State University,
Normal, IL, USA

Keywords
Toxic Waste · Flint · MI · Love Canal · Environmental Justice

Definition

The issue of toxic waste and residences includes incidents and policies related to the broader environmental justice and antitoxic movements in the United States, including "NIMBY" (Not In My Backyard), health effects, and considerations of environmental racism.

Introduction

On the South Side of Chicago lies a federal housing project, originally created for African-American veterans. Nicknamed the "toxic doughnut," it has the highest concentration of hazardous waste sites in the nation, being surrounded by 50 landfills and 382 industrial facilities, with 250 leaking storage tanks underground (Cosier 2017). Studies have revealed dangerous levels of toxic chemicals in the area, with the community having the highest cancer rates in the city (Cosier 2017; Taylor 2000; Wenzel 1998). Since industrialization began in modern America, we have seen issues of toxic waste and how it affects communities unfold repeatedly. With the inception of the antitoxic and environmental justice movements, communities have and continue to grapple with issues of toxic waste near their homes and the consequences of such environmental hazards.

Love Canal: The Beginning of the Antitoxic Movement

The toxic waste disaster at Love Canal in the late 1970s garnered attention and galvanized grassroots environmental justice movements. Between 1942 and 1953, Hooker Chemical Corporation filled a canal with 21,800 t of chemical waste in the city of Niagara Falls, New York. Despite this, the site was later sold to the Niagara Falls school board for one dollar and included a deed with a provision that relieved Hooker Chemical of any future liability. Years later, after the drums of chemicals had gradually corroded, the contents leached through the soil into the basements and backyards (Levine 1982). Residents had complained of strong odors and substances around their homes for years prior. Children had complained of burning feet while barefoot in their yards, along with unexplained skin irritations (Silveira 2000). After a winter storm in 1977, with a rising water table, the toxic waste flowed out into the backyards of residents. By the time citizens were aware of the threat of chemicals, serious consequences had potentially already occurred (Levine 1982). By 1978, this was national news and considered a disastrous environmental tragedy.

Members of the community took action, led by Lois Gibbs of the Love Canal Homeowners Association. Gibbs' son had respiratory problems after attending the school built on top of a toxic waste disposal (Silveira 2000). Frustration with government officials was paramount as the community protested, alleging that the Niagara County Health Department and other officials had known about the problems in Love Canal and ignored them. The residents of the association developed a community health survey, confronted politicians, and protested (Silveira 2000). It was eventually recommended that pregnant women and children under the age of 2 relocate. In the end, the federal government bought out the homes of hundreds of families and the residents left.

Ultimately, Love Canal became a catalyst for the antitoxic movement, as well as the creation of the Superfund through the Environmental Protection Agency, which is a program to fund the cleanup of the most contaminated and toxic sites in the country. Prior to this incident, toxic waste was not an issue seen as a serious threat to communities. This changed after Love Canal. By 1980, America feared toxic waste just as much as they had feared nuclear power after the Three Mile Island meltdown, and concerns about toxics led to the development of social movement organizations (Szasz 1994).

The antitoxic groups developed underneath the broad definition of the environmental movement, concerned with the effects that waste have on people, including their own families. Initially considered a movement of housewives, motivated women with little political knowledge became

activists (Silveira 2000). As the movement grew, the government eventually established the Center for Health, Environment, and Justice (formerly known as Citizen's Clearinghouse for Hazardous Wastes) in 1981.

This event, like many others, began as a "Not In My Backyard" problem – otherwise called "NIMBY." These groups are locally formed antitoxics groups created in reaction to perceived local health risks to families and communities (Silveira 2000). Residents were troubled by the public health repercussions from possible groundwater contamination, especially since this occurred in the aftermath of Love Canal (McGurty 1997). It eventually became apparent that toxic waste could threaten everyone; it was always a present danger (McGurty 1997).

The National Toxics Campaign and other social organizations were created to address the issue in people's backyards that was gaining attention. Critics were quick to label many involved with these organizations as NIMBYs, who were not concerned about where the toxic waste ended up as long as it was not near them. This was largely a sweeping that did not apply to the vast majority of those in the movement who did indeed push for the reduction of toxic waste everywhere. By the 1980s, social justice-oriented movements were becoming enmeshed with environmental causes, ultimately leading to the concept of environmental justice.

The Environmental Movement

The modern environmental movement began after Rachel Carson's publication of *Silent Spring* (1962), which focused on toxics harming the environment and wildlife. Prior to this time, the environmental movement was primarily concerned with conservation. Gunter and Kroll-Smith (2007) identified the three prominent types of environmental conflict as conservancy disputes, siting disputes, and exposure disputes. Conservancy disputes are struggles over how to define and protect natural areas and species. Siting disputes characterize what happens when conflict arises over some proposed land use, and exposure disputes involve fights against hazards already present in a community. Siting and exposure disputes are particularly salient where toxic waste is concerned.

The environmental justice movement has adopted a model of science as embedded in social structures. Environmental conflicts arise when a community exposed to a hazard makes connections between their health and the hazard in their community (Hannigan 2006). Allen (2003) describes this with a particular scenario on popular epidemiology. A woman by the name of Robinson established a health registry in her Louisiana community, making maps to track various illnesses and their proximity to Superfund sites and chemical industries to prove causation. This is a heavily contested issue in environmental movements, because causation tends to be ambiguous and extremely difficult to prove. Indeed, public health has become a major concern, as have efforts to hold hazardous chemical sites and corporations accountable.

The environmental justice frame was built around a concept of rights constructed by the rhetoric of previous social movements (Čapek 1993). Four major components of the environmental justice discourse were identified by Čapek (1993). All citizens have a right to obtain accurate information about the situation, a serious unbiased hearing when contamination claims are made, democratic participation in deciding the future of the community that has been contaminated, and compensation from those who have inflicted harm and polluted a community (Čapek 1993; Hannigan 2006). The concentration and dependence on the legal system to compensate victims of environmental wrongdoings and to hold accountable those who committed those wrongdoings are built into the framework for environmental justice movements.

Additionally, the environmental justice movement has a framework for social change that includes the principles that all individuals have the right to be protected from environmental hazards and degradation. It also adopts a public health model of prevention which focuses on the elimination of a threat before the harm occurs, shifts burden of proof to the polluters, and redresses

disproportionate risk burdens (Brulle and Pellow 2006). This is in line with the precautionary principle, which means that rather than presuming possible hazards are safe until data proves otherwise would mean allowing scientific uncertainty to delay action, so the burden is shifted to instead show an actual absence of harm (Brulle and Pellow 2006; Hannigan 2006).

We can look to the example of grievances and environmental justice as described by Čapek (1993) and his case study of the Carver Terrace neighborhood in Texas. The grievances that led to this environmental movement in the community began with health problems, which residents claimed were the result of contamination in their neighborhood by the corporation Koppers Texarkana. This led to more people becoming involved and turning to the judicial system for justice. Their claims were considered valid, as the Environmental Protection Agency had become aware of the problem many years prior, and declared Koppers Texarkana a Superfund site (Čapek 1993).

Illnesses related to environmental hazards can lay dormant for years. This is why some argue we have yet to see the full effect of toxic waste on public health (Brulle and Pellow 2006). With the passage of the Superfund Act and the 1986 Emergency Planning and Community Right-to-Know Act, the movement gained momentum for using government funds to clean up hazardous sites and give citizens more power.

The Chemical Corridor

The civil rights movement of the 1960s and the environmental movement of the 1970s ushered in the era of environmental justice in the 1980s, particularly in poor and minority communities that recognized the disproportionate amount of hazardous waste located where they lived (Allen 2003). In 1989 the environmental justice movement gained momentum in Louisiana, when residents organized the first Great Louisiana Toxics March to bring attention to the illnesses and industrial pollution in their communities, located within the chemical corridor (Allen 2003). The commercial development of this area was ushered in by the wealthy few with power and the enticing corporate-friendly environment by a government that required no property taxes and was near a water supply – the great Mississippi River. This area is home to many chemical corporations and involves both siting and exposure conflicts (Allen 2003). Though called the Chemical Corridor by many, to others it is known as Cancer Alley, or Death Alley, representing a range of fatal illnesses that struck the communities along the river. Other signs of powerlessness are ever present. Loudspeakers are posted on telephone poles to sound alarms and warn residents in the event of a chemical leak.

In Louisiana, companies had to apply for separate permits based on whether it polluted the air, water, or ground. This three-media permit system allowed corporations to creatively hide pollution and toxics (Allen 2003). At public hearings for permits regarding toxic waste, resident concern and questions were only fielded if they addressed the permit application directly (Allen 2003).

The work of expert-activists became essential to the Louisiana movement. Expert-activists inform residents of the scientific knowledge, laws, and regulations related to their rights with regard to environmental issues. These individuals became teachers for the residents to help them explain their experiences in ways that would help them gain legitimacy in public policy. The citizens needed to have a basic understanding of toxic waste and its effects, and they needed to understand the process by which they might initiate change. The production and distribution of information was an important goal. One community group – Save Our Selves – filed a lawsuit again the Louisiana environmental control commission and the Department of Natural Resources and, eventually, won (Allen 2003). The state supreme court decided that citizens' environmental protections must be considered equally with economic and social factors. After this, corporations wanting to site their facility in the corridor had to demonstrate that they had considered alternative sites and proposed the most advanced pollution control processes to mitigate harms. While toxic waste would still be some concern, the

benefit of economics and jobs would remain in this "industrial corridor," so-called by government officials attempting to emphasize economic advantages for citizens. These advantages are misleading, because the jobs require specific skill sets that unskilled workers cannot occupy. For the state, the chemical corporations exemplify a capital investment.

Environmental Racism and Siting of Toxic Facilities

In Warren County, North Carolina, an environmental hazard was brewing in 1982, leading to the first large-scale civil disobedience within the environmental justice movement. Warren County was a predominately African-American community selected for a landfill to dump PCB-contaminated waste. When residents became aware, they blocked the trucks from entering the site. Ultimately, this drew attention to how environmental toxics affected minority communities, and environmental racism began to gain attention.

Bullard (1990) defined environmental justice as the principle that all people and communities are entitled to equal protection under environmental and public health regulations. Bullard used this frame in his work *Dumping in Dixie*, which examined five communities in the South and the activism and mobilization strategies of black residents who were confronted with environmental hazards. In each of the states where Bullard researched case studies, the population of black residents was around 30%. However, in communities where hazardous waste and dumping sites were found, the black and minority population was at least 90% (Bullard 1990). Bullard's work became the first in-depth study of environmental racism. Environmental racism refers to discrimination in environmental policymaking (Brulle and Pellow 2006). In 1987, the United Church of Christ Commission on Racial Justice released a study titled *Toxic Waste and Race in the United States*. This study, as well as Bullard's research, definitively outlined how black and other minority communities were singled out for hazardous waste sites and how they used the environmental justice frame to organize collectively.

Environmental racism is racial discrimination in environmental policymaking, the enforcement of regulations and laws, the deliberate targeting of communities of color for toxic waste facilities, the official sanctioning of the life-threatening presence of poisons and pollutants in our communities, and the history of excluding people of color from leadership of the ecology movements (Brulle and Pellow 2006).

Bullard traced the environmental justice movement in the communities he studied all the way back to the civil rights movement. The civil rights movement provided a master frame that validates the struggle for rights by other disenfranchised groups (Bullard 1990; Čapek 1993). Churches in the communities Bullard studied were a major catalyst in organizing community members. Just as in the civil rights movement, many important figures of the movement were community leaders who stood up for their rights despite not having the resources to advance their cause (Bullard 1990). In these ways, the civil rights movement shaped the environmental justice movement in the black community. Environmental justice can be distinguished from environmental inequality, which refers to a situation in which a specific social group is disproportionately affected by environmental hazards.

Class has been said to play a role in siting of toxics as well. Studies have demonstrated that the poor and minorities face a disproportionate burden of exposure to environmental health hazards and toxics (Brulle and Pellow 2006). Evans and Kantrowitz (2002) found that there is a relationship between ethic and class characteristics of a community and levels of exposure. Other studies found that in some areas of the country, specifically Southern California, race was not only a strong predictor of siting facilities, but it also explained cancer risk distributions even when controlling for other demographics (Brulle and Pellow 2006). The social dynamics that create and allow environmental inequality to function are the economy and institutionalized racism.

As industrialization expanded and became modernized, the dangers and consequences were

unforeseen. Corporations were concerned only with profits. Polluters argued for siting in locally unwanted land uses (LULUs) because they have less political power and ability to resist. As the environmental justice movement grew throughout the 1980s, many groups organized around minority and poor communities, as these were the places more heavily burdened with toxic waste and pollution (Brulle and Pellow 2006). These community organizations built a framework for social justice that included the following: the right of all individuals to be protected from environmental degradation, public health model of prevention as the primary strategy to prevent harms, shifting burden of proof to the offending entity, allowed disparate impact and statistical weight, and redresses risk through targeted action (Brulle and Pellow 2006).

Even today, lead poisoning continues to be the number one environmental health threat to children in America, disproportionately affecting poor and minority children (Bullard et al. 2008). Black children are five times more likely to suffer lead poisoning, and one in seven black children living in older inner-city housing has elevated lead levels (Bullard et al. 2008). Minorities not only suffer worse consequences from pollution and toxics, but they receive disparate treatment at the hands of the government when attempting to fight against pollution and toxic waste.

Native Americans are also at high risk from toxic threats and the siting of waste facilities near residences (Brook 1998). Native Americans live at the lowest socioeconomic level in the United States. Their lands have been targeted by the government for hazardous waste sitings. One study found that of the 110 commercial nuclear power plants, the government has solicited every tribe, offering millions of dollars for them to host a waste facility (Angel 1991; Brook 1998). This "toxic trade" is appealing to impoverished communities. The categories of people who illegally dump waste on the native land have been referred to as midnight dumpers and native entrepreneurs (Brook 1998). Midnight dumpers are outsiders who do so secretly and illegally. Native entrepreneurs are members of the tribe who stand to gain profit. Ultimately, as Szasz (1994) wrote, "the intersection of race discrimination and exposure to toxic hazards is one of the core themes of the anti-toxics movement" (151).

Toxic Waste Concerns

Concern over toxic waste frequently begins with local citizens who come to draw a causal link between seeping dump sites and a perceived increase in the neighborhood incidence of health problems (Hannigan 2006). Toxic waste sites affect millions of Americans, and two million people live within a mile of a Superfund site, some of the most toxic areas (Laurian 2004). Issues with toxic sites also create environmental and public health risks, stigmatize communities, and affect land use (Laurian 2004). By 2016, approximately 53 million people lived within 3 miles of a Superfund site which is equal to 16% of the US population (EPA 2017). The current data on the EPA website lists 1342 National Priority List Superfund sites. Hazardous waste that is not properly managed could cause adverse health effects on the population within the vicinity (Fazzo et al. 2017).

Krieg (1998) argued that the siting of toxic waste facilities was based on community tax structure and socioeconomic standing of the community in question. Tax structures may affect how dependent a community is on maintaining resources and businesses in the area for investment. As has been argued in other areas of the nation, the need for economic development is a great consideration here. Working-class communities are more affordable land and more favorable political climates for industrialization. In this, Krieg argues that the toxic waste crisis is becoming suburbanized. In his analysis of 44 towns, working-class neighborhoods faced greater siting risks than middle-class towns. One conclusion to be drawn is that environmental movement activity creates conditions unfavorable to capital accumulation and pushes toxic waste producing industries into other areas (Krieg 1998).

Although it is possible for chemicals to migrate off-site from landfills, there is not much known on the extent to which citizens living near landfill

sites are exposed to chemicals (Vrijheid 2000). For example, there were studies done that followed the contamination of two drinking-water wells in Santa Clara County, California, with chlorinated solvents that had leaked from an underground waste storage tank. Near one of these sites, there were reports of a cluster of adverse pregnancy outcomes (Vrijheid 2000). As is true for many public health issues tied to environmental hazards and toxic waste, effects of the exposure for the population are difficult to establish. Several studies suggest a relationship between proximity to landfill sites and adverse pregnancy outcomes. Single-site studies focusing on one landfill and community demonstrate an increase in infants with low birth weight, which is considered to be a marker of the effects of chemical exposure. Multi-site studies are too few to determine further health consequences, though birth defects have been reported, but it is difficult to establish causality. This is especially true for cancers, as evidence for a causal relationship between landfill exposure and cancer is weak, and there are long latency periods (Vrijheid 2000). Proof of causation in the case of cancer and suspected environmental hazard-related diseases is very difficult. This proved to be the case in Louisiana's chemical corridor as well, as epidemiology studies have failed to prove or disprove what many residents strongly believe, that their constant exposure to toxic waste and hazardous materials causes cancer and death (Allen 2003).

Other research examines the proposition that since the growing public concern and opposition to waste facilities, siting follows the path of least political resistance, resulting in environmental inequality. Saha and Mohai (2005) performed a longitudinal analysis on Michigan over 30 years and found patterns of disparate siting for facilities after 1970. Because Love Canal put toxic waste exposure on the radar of many Americans, it also heightened fears that other neighborhoods were unknowingly at risk and added fuel to the NIMBY phenomenon (Saha and Mohai 2005). The antitoxic movement took hold in many middle- and working-class neighborhoods, and citizen involvement increased as a result.

Flint and the Water Crisis

In 2014, Flint, Michigan, began to experience an ongoing water crisis. The drinking water source for the city was switched from Lake Huron to the Flint River, a more cost-effective water supplier. This was done in anticipation of a $25 million deficit, while the city constructed a new pipeline (Reilly 2017). The water was insufficiently treated, and the city announced the presence of bacteria as lead had leached into the drinking water. A state of emergency was declared in 2016, and residents were informed to use bottled or filtered water only. Residents experienced a series of health effects from lead contamination. Government officials initially denied that there were problems and refused to go back to the original supplier, even though it was common knowledge that Flint River was greatly polluted (Reilly 2017). Doctors conducting research found that the percentage of children in Flint with lead poisoning had doubled in 2015 (Gupta et al. 2016).

The incident is reminiscent of the Hinkley, California hazardous waste event, when Pacific Gas and Electric Company dumped millions of gallons of chromium-tainted wastewater into unlined water reservoirs during the 1950s and 1960s. It was absorbed into the groundwater, and after extended litigation in the 1990s, the issues with wastewater and pollution continue even today.

There is an ongoing environmental toxic contamination in today's world (Miller and Wesley 2016). Through congressional testimony on the incident, the public heard about deals that resulted in the poisoning of households. To that end, some have argued that the Flint water crisis is a form of violent assault against residents (Miller and Wesley 2016). The fear of ongoing health consequences that may lie dormant is a constant source of anxiety for victims of toxic exposure. Social trust is damaged beyond repair, and citizens lose any faith in government officials. Any sense of safety at home is lost and changed. Lead contamination is a serious health issue. As Miller and Wesley (2016) write, "in light of biopolitical considerations of lead poisoning risks, it is important to consider

who bears the risks for decisions made without social consent of those governed, to identify how risks and uncertainty, with their associated costs, are distributed throughout communities, and address the restorative responsibility link between the public and private spheres" (74).

Conclusion

Disasters that result in toxic contamination disrupt the social fabric of the communities where they happen (Miller and Wesley 2016). As industrialization and technological advancements increase in society, we are left at risk to toxic waste and hazards. While various social movements have garnered attention for environmental hazards and toxic waste in households, the water crisis in Flint, Michigan, demonstrates this is an ongoing battle, where minority and poor communities still suffer a disproportionate impact and corporations are not held liable for their pollution and improper waste disposal, continuing to put communities at risk.

Cross-References

- ▶ Hazardous Environmental Effects
- ▶ Human-Made Disasters: Toxic Waste and Residences
- ▶ Investigations: Environmental Pollution Dumping

References

Allen, B. L. (2003). *Uneasy alchemy: Citizens and experts in Louisiana's chemical corridor disputes*. Cambridge, MA: MIT Press.

Angel, B. (1991). The toxic threat to Indian lands. *A Greenpeace Report*. Retrieved 25 Apr 2010.

Brook, D. (1998). Environmental genocide: Native Americans and toxic waste. *American Journal of Economics and Sociology, 57*(1), 105–113.

Brulle, R. J., & Pellow, D. N. (2006). Environmental justice: Human health and environmental inequalities. *Annual Review of Public Health, 27*, 103–124.

Bullard, R. D. (1990). *Dumping in Dixie: Race, class, and environmental quality*. Boulder: Westview Press.

Bullard, R. D., Mohai, P., Saha, R., & Wright, B. (2008). Toxic wastes and race at twenty: Why race still matters after all of these years. *Environmental Law, 38*, 371–411.

Čapek, S. M. (1993). The "environmental justice" frame: A conceptual discussion and an application. *Social Problems, 40*(1), 5–24.

Carson, R. (1962). *Silent spring*. Boston: Houghton Mifflin Harcourt.

Cosier, S. (2017, April 17). What a gutted EPA could mean for Chicago's 'Toxic Doughnut'. Retrieved from https://www.nrdc.org/stories/what-gutted-epa-could-mean-chicagos-toxic-doughnut

Environmental Protection Agency. (2017). Population surrounding 1,836 Superfund remedial sites. Retrieved from https://www.epa.gov/sites/production/files/2015-09/documents/webpopulationrsuperfundsites9.28.15.pdf

Evans, G. W., & Kantrowitz, E. (2002). Socioeconomic status and health: The potential role of environmental risk exposure. *Annual Review of Public Health, 23*(1), 303–331.

Fazzo, L., Minichilli, F., Santoro, M., Ceccarini, A., Della Seta, M., Bianchi, F., Combam, P., & Martuzzi, M. (2017). Hazardous waste and health impact: A systematic review of the scientific literature. *Environmental Health, 16*(1), 107.

Gunter, V., & Kroll-Smith, S. (2007). *Volatile places: A sociology of communities and environmental controversies*. Thousand Oaks: Pine Forge Press.

Gupta, S., Tinker, B., & Hume, T. (2016). 'Our mouths were Ajar': Doctor's fight to expose flint's water crisis. *CNN*. Retrieved 15 July 2016.

Hannigan, J. (2006). *Environmental sociology*. London: Routledge.

Krieg, E. J. (1998). The two faces of toxic waste: Trends in the spread of environmental hazards. *Sociological Forum, 13*(1), 3–20. Kluwer/Plenum Publishers.

Laurian, L. (2004). Public participation in environmental decision making: Findings from communities facing toxic waste cleanup. *Journal of the American Planning Association, 70*(1), 53–65.

Levine, A. G. (1982). *Love Canal: Science, politics, and people*. Lexington: Lexington Books.

McGurty, E. M. (1997). From NIMBY to civil rights: The origins of the environmental justice movement. *Environmental History, 2*, 301–323.

Miller, D. S., & Wesley, N. (2016). Toxic disasters, biopolitics, and corrosive communities: Guiding principles in the quest for healing in Flint, Michigan. *Environmental Justice, 9*(3), 69–75.

Reilly, C. M. (2017). Potable to poisonous: An analysis of the Flint, Michigan water crisis. *Senior Honors Projects, 2010-current*. 338. http://commons.lib.jmu.edu/honors201019/338

Saha, R., & Mohai, P. (2005). Historical context and hazardous waste facility siting: Understanding temporal patterns in Michigan. *Social Problems, 52*(4), 618–648.

Silveira, S. J. (2000). The American environmental movement: Surviving through diversity. *Boston College Environmental Affairs Law Review, 28*, 497.

Szasz, A. (1994). *Ecopopulism: Toxic waste and the movement for environmental justice* (Vol. 1). Minneapolis: University of Minnesota Press.

Taylor, D. E. (2000). The rise of the environmental justice paradigm: Injustice framing and the social construction of environmental discourses. *American Behavioral Scientist, 43*(4), 508–580.

United Church of Christ Commission for Racial Justice. (1987). *Toxic wastes and race in the United States: A national report on the racial and socio-economic characteristics of communities with hazardous waste sites*. New York: Public Data Access.

Vrijheid, M. (2000). Health effects of residence near hazardous waste landfill sites: A review of epidemiologic literature. *Environmental Health Perspectives, 108*(Suppl 1), 101.

Wenzel, L. (1998). Hazel Johnson. *On The Issues, 7*(1), 30.

Further Reading

Benz, T. A. (2017). Toxic cities: Neoliberalism and environmental racism in Flint and Detroit Michigan. *Critical Sociology*. https://doi.org/10.1177/0896920517708339.

Brown, M. H. (1981). *Laying waste: The poisoning of America by toxic chemicals*. New York: Washington Square Press.

Edelstein, M. R. (1988). *Contaminated communities: The social and psychological impacts of residential toxic exposure*. Boulder: Westview Press.

Industrial Control System

Marie-Helen Maras
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Industrial control system · Critical infrastructure

Definition

An industrial control system is a general term used to describe systems that are designed to monitor, oversee, manage, and/or support processes of critical infrastructure.

Introduction

An industrial control system is a general term used to describe systems that are designed to monitor, oversee, manage, and/or support processes of critical infrastructure (i.e., "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety"; DHS n.d.). The United States has 16 designated critical infrastructure sectors (CISA n.d.): chemical; commercial; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater. These critical infrastructures are both publicly and privately owned. The vast majority of critical infrastructure sectors, however, are privately owned (FEMA 2011). This private ownership complicates efforts to harmonize measures designed to protect and secure the ICS of these sectors from cybersecurity threats and vulnerabilities.

Cybersecurity Threats and Vulnerabilities

Industrial control systems are vulnerable to internal cybersecurity threats and external cybersecurity threats that could compromise or exploit the confidentiality (i.e., prevention of unauthorized access), integrity (i.e., preservation of the accuracy and trustworthiness of data), and availability (i.e., accessibility) of systems, networks, services, and data (Maras 2016; UNODC 2019). Internal threats, like insider threats, are those posed and committed, in whole or in part, by individuals within an organization or agency, who have authority, access, and/or privileges

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

within an organization/agency to, for example, steal data or engage in sabotage (e.g., modifying data or damaging systems). ICS are also vulnerable to external threats, predominately because they were not originally built with cybersecurity mind.

ICS were previously made up of isolated systems and separate networks. The original systems were primarily secure systems protected against cybersecurity threats – at least remote unauthorized access to these systems. Today, however, this has changed. ICS are now networked to increase efficiency of operations and facilitate the sharing of real-time information about their operations. This networking enables the remote access of ICS and exposes these systems to cybersecurity risks. ICS are, thus, vulnerable to external cybersecurity threats because of their design and operations.

Certain ICS are still legacy systems – proprietary systems that do not contain standard architecture and syntax (DHS 2016; Stouffer et al. 2015). This is both a negative and a positive feature of ICS. It is a negative feature because proprietary systems are often hard to manage and operate as they require specialized knowledge. It is a positive feature because perpetrators, who learn the inner workings of these systems and gain access to them, cannot use this knowledge to gain access to other industrial control systems. Other ICS are off-the-shelf or standardized (DHS 2016; Stouffer et al. 2015). Off-the-shelf ICS are used because they cost less than proprietary and legacy systems and are easy to use, making them more effective and efficient to manage and operate. Nevertheless, off-the-shelf ICS afford perpetrators with the opportunity to learn about the inner workings of these systems and to gain unauthorized access to them. These perpetrators can then use this knowledge or share this knowledge with others, to gain unauthorized access to other off-the-shelf ICS used in similar or different critical infrastructure sectors. Because these systems could be located in different parts of the world with varying degrees of security, perpetrators can access these systems from countries and/or facilities that are not well protected and can use the knowledge gained from this unauthorized access to target other countries.

Securing ICS

Practical strategies for achieving security of industrial control systems include risk management; physical security measures (e.g., access controls and security guards); personnel security measures (e.g., background investigations and robust recruitment, hiring, selection, and retention policies); network and security architecture (e.g., network segmentation and "specific controls and their strategic placement within the network or systems to establish layers of security"); host security (e.g., ICS update and patch management and strong authentication measures); and security monitoring (e.g., audit logs that provide information about user activity, such as files access, modification, download, and/or removal, and other activities, intrusion detection systems, and intrusion protection systems) (DHS 2016, pp. 4–34). Vendor management and vendor security are also integral facets of securing ICS (DHS 2016). Here, vendors, their products, and services should be properly vetted and monitored to not only ensure the quality of goods and services but also to verify that cybersecurity policies, procedures, and practices are followed by vendors. Supply chain compromises in the form of software or hardware with malware and vulnerabilities in software applications have brought home the lesson that attention needs to be paid to this area. Finally, clear ICS security policies and procedures, as well as policies and procedures on the misuse of ICS, are also needed and should be communicated to all ICS employees (DHS 2016). ICS owners, users, and, to the extent that it relates to them, vendors, should also receive training on these policies and procedures (DHS 2016).

Conclusion

Industrial control systems are vulnerable to cybersecurity threats. To protect ICS, measures are needed to detect cybersecurity threats, restrict unauthorized access to ICS, and protect ICS from misuse and criminal exploitation. The type of security measures chosen, however, depends on the type of ICS.

Cross-References

- Critical Infrastructure Protection
- Critical Infrastructure: Commercial Facilities Sector
- Critical Infrastructure: Critical Manufacturing Sector
- Critical Infrastructure: Defense Industrial Base Sector
- Critical Infrastructure: Emergency Services Sector
- Critical Infrastructure: Government Facilities Sector (GFS)
- Critical Infrastructure: Nuclear Reactors, Materials, and Waste Sector
- Critical Infrastructure: Transportation Systems
- Critical Infrastructure: Water and Wastewater Systems Sector
- Insider Threat
- SCADA

References

CISA. (n.d.). Critical infrastructure sectors. https://www.cisa.gov/critical-infrastructure-sectors.

DHS. (2016, September). Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies industrial control systems. Cyber Emergency Response Team. https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

DHS. (n.d.). Critical infrastructure security. https://www.dhs.gov/topic/critical-infrastructure-security.

FEMA. (2011). Critical infrastructure: Long-term trends and drivers and their implications for emergency management. Office of Policy & Program Analysis (OPPA). https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

Maras, M.-H. (2016). Cybercriminology. New York: Oxford University Press

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). NIST special publication 800-82 revision 2. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf.

UNODC. (2019). Module 2 ~ General Types of Cybercrime: Offences against the confidentiality, integrity and availability of computer data and systems. E4J Cybercrime Modules. https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

Further Reading

DHS. (2016, September). Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies industrial control systems. Cyber Emergency Response Team. https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). NIST special publication 800-82 revision 2. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Influence of Risk Perception on Event Risk Management and Decision-Making

Peter Ashwin
Event Risk Management Solutions, Boise, ID, USA

Keywords

Risk Management · Event Management · Risk Perception · Risk-based Decision-making

Introduction

In today's global risk society, event organizers find themselves in an environment characterized by diverse and dynamic risks ranging from home-grown violent extremism, cyber-threats, event cancellations due to severe weather, and a saturated market which offers locals and visitors a diversity of competing events to choose from Berlonghi (1990), Tarlow (2002), Rutherford Silvers (2008), and Piekarz et al. (2015). Due to the serious impacts from these issues and incidents, risk management should be viewed by event organizers as a fundamental responsibility for planning and delivering safe and secure events (Rutherford Silvers 2008). Furthermore, a rational and structured approach to risk management will enhance the event organizers' ability to make appropriate decisions within fast-paced, complex,

and uncertain environments (Hillson 2016). However, risk management is also prone to subjectivity, bias, and error leading to exaggeration and overestimation or underestimation of risk which may result in ill-informed decisions (Lupton 2013).

It is sometimes said that risk management is too subjective. To what extent is this true and what are the implications for event organizers? This entry will critically analyze whether risk management within the events industry is too subjective and if subjectivity positively or negatively influences the effectiveness of decision-making.

First, the interconnected concepts of risk management, uncertainty, and subjectivity must be defined to form the basis to explore whether risk management is rational and objective or, conversely, subjective. Second, the theoretical perspectives underpinning risk perception will be analyzed to explore how these sociocultural perspectives may influence whether a rational or subjective approach to risk management is more effective for event organizers. Third, a critical analysis of whether the effectiveness and credibility of risk-based decisions by event organizers is positively or negatively influenced by their perception of risk and their organizational culture. Fourth, the notion of risk-based decision-making by event organizers will be examined to identify how event organizers identify with and respond to risk within today's global risk society (Beck 2006).

Finally, it will be noted that despite the gaps in evidence and literature on event risk management (Khir 2014; Robson 2009), this entry will argue that the risk management approach adopted by event organizers is primarily subjective; however, this approach does not negatively impact their decision-making ability under ambiguous conditions. Moreover, it will be argued that if event organizers adapted their subjective approach with a rational approach to risk management, this combined risk-based decision-making process would enhance their organizational capability to prepare for, respond to, and recover from adverse risk events (Talbot and Jakeman 2009).

Managing Risk in Today's Uncertain World

Today's global risk society is volatile, uncertain, complex, and ambiguous (Beck 2006; McCaughey et al. 2017). National boundaries are blurred, and interconnected markets are exposed to delocalized risks with consequences that may stretch over extended or indefinite periods of time (Beck 1992, 2006). This section of the entry will explore the concepts of risk and event management to examine how risk management is considered by event organizers.

First, while there is no definitive or widely accepted definition of what an "event" is, an event can be best described as "an opportunity for leisure, social or cultural experience outside the normal range of choices or beyond everyday experience" (Getz 1997, p. 4). Furthermore, the events industry encompasses a diverse range of activities that includes festivals, parades, meetings, conventions, expositions, sport, and other special events. Within the industry, event organizers are responsible for the research, design, planning, coordination, and execution of events (Goldblatt 2011).

In order to understand how risk is managed, one must first explore the concept of risk. ISO 31000 (2018) describes risk as the consequence of an organization setting (ecosystem) and the pursuit of the achievement of their mission and objectives against an uncertain environment influenced by internal and external factors which the organization may not completely control (Purdy 2010, p. 882). While risk generally refers to undesirable events, risk also provides opportunities for an organization to achieve favorable outcomes in pursuit of their mission and objectives (Hopkin 2010). Moreover, when risks are effectively managed, the chances of achieving stated goals and objectives will be optimized (Hillson 2016).

Berlonghi (1990) was among the first academics to identify risk management as an integral part of the event management process: the process by which an event is planned, prepared, and produced (Goldblatt 2011; Rutherford Silvers 2008). Within the events context, risk management can

be described as the process of making and carrying out decisions that minimize the adverse effects of the potential losses of an event or simply stated as "making events as safe and secure as possible" (Berlonghi 1990, p. 3), or alternatively

> a comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision making for managing risks that may hinder an organization from achieving its objectives. (US Department of Homeland Security 2011, p. 13)

While there is a relatively large body of literature asserting that risk management is fundamental to planning and delivery of safe and secure events, there remains a gap in research and literature specific to event risk management (Khir 2014; Robson 2009). Furthermore, it is also noted that the existing body of literature on risk management within the events industry focuses in most part on insurance and legal obligations, typically agreements, indemnifications, and waivers (Rutherford Silvers 2008).

Effective risk management requires the assessment of inherently uncertain events through two dimensions: (1) how likely is the risk event and (2) what is the impact to the organization's objectives? The probabilistic risk assessment (PRA) is one of the most commonly used tools to quantify risk through an assessment of the aforementioned factors of likelihood (probability) and consequence (Ostrom and Wilhelmsen 2012).

Talbot (2011) argues that if sufficient rigor has been put into defining the context of the risk statement, the likelihood, and the consequence metrics, then a meaningful risk estimate (risk rating) can be quickly and consistently obtained from a risk matrix. Although semiquantitative in nature, risk matrices provide a focus for decision makers to identify and manage the highest priority risks and provide a simple visual presentation of these ranked risks (Hopkin 2010).

Additionally, Talbot (2011) contends that the inherent limitations of risk-based decision-making within uncertain environments and the fundamental processes of human risk perception mean that the subjective decision-making will always be part of the risk assessment process. Following on from Talbot's argument, the next section of the essay explores the theoretical perspectives underpinning risk perception and how these sociocultural perspectives may influence the way event organizers identify and manage risk.

The Influences of Risk Perception and Heuristics

It can be said that event organizers' risk perception is not only based on perceptive or objective fact, but also by the individual's background, experience, and the organizational culture (Robson 2009). In following section of the essay, techno-scientific and sociocultural perspectives underpinning risk perception will be examined to explore how these perspectives influence an event organizers approach to risk management.

There are arguments on both sides over whether risk is subjective or objective or a combination of both, noting that there is an inevitable element of "subjectiveness" within human judgment and decision-making (Bradbury 1989, cited in Lupton 2013, p. 28). Subjectivity can be defined as the influence of personal beliefs or feelings, rather than facts (Cambridge English Dictionary 2016).

The phenomena of risk perception have been theorized in social scientific literature through three major perspectives: (1) the naïve realist or techno-scientific, (2) cognitive psychology, and (3) sociocultural (Lupton 2013, p. 26). The techno-scientific perspective contends that risk is a product of a hazard (or risk source) with calculations of likelihood and the consequences of a risk event (Lupton 2013, p. 27). The underlying premise is that risk can be measured and calculated which is also consistent with the approach outlined within ISO 31000 approach. One weakness of the techno-scientific theory is that the "lay person's perceived lack of risk knowledge and how their response to risk is based on inferior and unsophisticated sources of knowledge such as intuition" (Lupton 2013, p. 28). Counter to this argument, Wynne (1989, cited in Lupton 2013, p. 148) argues that lay persons' assessment of risk

incorporates their preestablished knowledge of how relevant industries and regulatory bodies have tended to deal with risk in the past. This position is supported by the social-constructionist argument that risk judgments are in part based on prior knowledge, personal embodied experiences, discussions with others, and access to expert knowledge (Lupton 2013, p. 45).

Like other lay persons, event organizers often rely on intuitive risk judgments (risk perception) to explain responses to risk. Rogers (1997) argues that risk perception rests on a foundation of overall experience which seldom incudes direct experience with the risk event. Within the events environment, risk perception has been described by Berlonghi (1990, p. 19) as being "the concerns of the various entities involved in the event" and that the risks identified by the event organizers may not be accurate nor verifiable, particularly if in the absence of an event risk assessment. Given their shortfall in experience with risk events, event organizers often rely on industry associations like the International Festival and Events Association (IFEA) to gain

> a shared, accumulated experience to determine which foreseeable losses are most probable, losses which are the most harmful and which harms (risks) may be preventable to assess and manage risk based on their previous risk event experience or that of other event organizers. (Douglas 1985, cited in Lupton 2013, p. 54)

One heuristic process that has special relevance for risk perception is known as "availability" bias (Tversky and Kahneman 1973 cited in Slovic 2000, p. 105). Event organizers intuitively use this process to judge an event as likely or frequently occurring, if the circumstances are easier to recall or have been experienced. Frequently occurring events are generally easier to recall than a rare event. In the absence of documented risk management plans (Robson 2009; Blerter and ERMS 2019), it is inferred that the majority of event organizers rely on intuitive risk judgments to manage their organizational and event risks. There is also an argument that an individual's risk perception could be changed, should additional information be available (Rogers 1997).

Event Organizers Approach to Risk Management

Event organizers seldom have statistical evidence or supporting event data (Robson 2009) to make informed judgments on the likelihood and consequences of risk. This is due to event organizers' lack of event documentation (after-action reports, near miss, and incident reports) which provide risk insights and proactive information on the effectiveness of the risk control environment (Reason 1997). In the most part, event organizers rely on their collective organizational memory to make inferences and decisions based on what they remember observing or experiencing during previous risk events; this heuristic process is referred to as judgmental bias (Slovic 2000). Based on this inference, it can be argued that event organizers use heuristics to make risk-based decisions in fast paced, uncertain environments. This opinion is supported by Slovic (2000, p. 41) who argues that people may judge risk and the benefits of hazards more efficiently under time pressure using heuristics rather than analytical processing and that human judgment is needed to interpret risk information and findings to determine the risk estimate.

Event organizers proactively seek out information on risk to support their risk judgment for identifying and selecting an appropriate course of action to avoid or mitigate the identified risk phenomena for their event or organization (Robson 2009). Furthermore, as a lay person, an event organizer's subjective response to risk should not be considered erroneous or biased if their opinions differ from that of expert risk assessments (Lupton 2013). The effectiveness and credibility of this subjective risk management approach will be further examined in the next section.

It is argued that scientific reasoning and experience are not mutually exclusive and that both should contribute to a rational assessment process that informs judgment that considers the totality of risk in a global risk society (Young 1995, cited in Lupton 2013). In this section, the level of subjectivity within the event organizers risk management approach will be further examined to determine whether it positively or negatively

influences their perception of risk or their approach to risk management.

There is an important contrast between the literature describing other for-profit business perception of risk as compared to the event organizers. For-profit businesses will willingly take risks in order to pursue opportunities to increase market share. In comparison, not-for-profit event organizers, the concepts of dread and the fear of the unknown have a profound influence on their perception of risk (Slovic 2000). Event organizers perceive risk as being negative and seek to avoid or reduce identified risks to a level as low as possible (Robson 2009). Furthermore, there is a common misperception amongst event organizers that insurance and legal documentation constitutes a risk management plan as compared to a structured approach like ISO 31000 which recommends documenting risk information within a risk register including the risk classification system, risk statements, risk owners, assessed risk levels etc. (ISO 2018; Piekarz et al. 2015).

While some techno-scientific theorists argue that a subjective approach to risk management is perceived as ineffective from a techno-scientific perspective, Beck (1999, cited in Lupton 2013, p. 80) argues that one should not have to choose between a natural-scientific objectivism (naïve realist) or a cultural relativism (subjective) approach for risk management, but rather use each when it is appropriate to understand the complex and ambivalent nature of the risk environment.

An example of this approach is Hancock's (2019) "forced risk ranking" approach which offers a simplified alternative to a PRA approach for ranking and prioritizing risks. Event organizers (including their operational line managers) are asked to identify their top ten risks within their organizational risk ecosystem, and then assign a numerical ranking value from one to ten to produce an aggregated score to rank and prioritize their risks. Hancock contends that the results from a forced risk ranking have shown much more separation among the risks, particularly when comparing results between different management groups (executives and managers). The other benefit of this approach is that there is no requirement to construct probability and consequence assessment scales to rank and prioritize risk. This simplified approach offers event organizers an opportunity to add process to their subjective risk assessments to better inform future decision-making and communication of risk information within the organization.

Decision-Making within the Events Environment

Talbot (2011) argues that subjective decision-making will always be part of the risk management process no matter what tool is used, and that these processes still effectively support risk informed decisions. In summary, there is insufficient evidence to suggest that a subjective risk management approach by event organizers is ineffective or lacks credibility. Following on, the next section will further explore decision-making processes by event organizers. Anecdotal evidence from a recent events industry survey conducted by Blerter and ERMS (2019) targeting CEOs and executive directors indicated only 17% of the 163 respondents were confident that their event team was mission ready, that is to say, operationally ready, organizationally resilient, and confident in their ability to respond to and make decisions under adverse and uncertain conditions. Event organizers, like other professionals, have great difficulty making decisions and judgments under uncertainty (Plous 1993). In this section, the concept of risk-based decision-making will be examined to identify how event organizers make decisions within uncertain and complex operating environments. As previously highlighted, there is little supporting evidence and literature on how event organizers (including senior leaders and operational managers) make risk-based decisions in situations that may involve consequences across multiple levels from individual to organizational to societal.

Rational theories of decision-making rest on the assumption that decision-makers follow a rational procedure for making decisions, selecting the option that will produce the best outcome (Laybourn 2003). While this rationale may be applicable in the military as part of the military

appreciation process in the selection of courses of action, this is not necessarily a common approach within the events industry. Are event management decisions driven by a deliberate and rational analysis or a more intuitive, heuristic-based approach to decision-making?

Given the current gaps in literature and scant research on event risk management and risk-based decision-making approaches by event organizers, literature on decision-making related to emergency first responders was reviewed for comparative analysis. The selection of this comparative analysis approach was based on the reasoning that both event organizers and first responders often operate within similar environments characterized by the requirement to make time critical decisions under uncertain conditions, constrained by availability of information.

Klein's (2008) recent research on recognition of prime decision model demonstrates that decision-making is a perpetual process, situationally based to facilitate fast effective decision-making, based on previous experience and intuitive knowledge that enables the decision-maker to generate fast and effective courses of action. The recognition primed decision model evidences that fast, effective decision-making is possible within time critical situations when the decision-maker has the expertise and situational awareness, combined with a battery of experience based, intuitive knowledge (Klein 2008). Similarly, research into naturalistic decision-making focused on how first responders utilized their expertise and experience to make effective decisions through utilizing systems of work known to have been successful in previous situations, often under uncertain and high stress situations (Ash and Smallman 2010). Event organizers like first responders will rarely have the necessary information and resources for an analytical based decision-making process (Tarlow 2002, p. 37), whereas the concept of "satisficing" is evidenced to more efficient under these conditions (Klein 2008).

It can be argued that the inherent limitations of event organizer's risk perception shape their decision-making under uncertain conditions, particularly given the influence of external "dread risks" over which the event organizer has no control. Event organizers risk perceptions of dread risks have become even more evident as a result of recent active shooter incidents which occurred at the 2018 Harvest 91 county music festival (Las Vegas) and the 2019 Garlic Gilroy Festival (California). Furthermore, evidence has shown that the individual event organizer's risk perception will always influence the subjectivity of the risk assessment process (Talbot 2011; Laybourn 2003). Additionally, research and literature on naturalistic decision-making provide a body of evidence that this decision-making approach is adaptable and viable for event organizers. Naturalistic decision-making allows event organizers to leverage their expertise, experience, and intuition to reach timely and effective satisficing decisions in fast-paced event environments.

Conclusion

In conclusion, controversy still remains whether risk management is too subjective. While it is acknowledged that event organizers approach to risk management is fundamentally subjective, it can be argued that these subjective risk assessments are equally rational as a scientific expert assessment (Lupton 2013). Event organizers construct their risk judgments based on insights from embodied risk experiences, organizational memory, and access to a collective industry body of risk knowledge shared through industry associations and other expert resources. While risk-related choices and decisions by event organizers are often driven by their subjective approach to risk management, this by no means indicates that this approach to risk management is ineffective or less credible. Nor is there any evidence to the contrary.

In light of the recent "dread" risk events that have recently occurred within the events environment, there is an increasing awareness among event organizers that a more structured approach to risk management is required to protect the value and reputation of their events and organization while pursuing their mission within an operating environment characterized by complexity and uncertainty (Rutherford Silvers 2008; Blerter and ERMS 2019). Similar to other organizations, there is also an increasing requirement for event

organizers to demonstrate an evidence-based approach to risk management with the ability to explain the rationale behind those decisions in clear, objective, and transparent terms (DHS 2011). However, in contrast, while most event organizers talk about risk, the majority of event organizers concede that they do not have a documented risk management plan for their event (Sturken 2005, cited in Robson 2009; Blerter and ERMS 2019).

In closing, while the evidence presented in this essay concludes that event organizer's risk management approaches are more subjective than rational and can be regarded as effective; event organizers must continue to seek opportunities to strengthen their current subjective risk management practices through a more objective approach based on international and industry risk management guidelines like ISO 31000. The future of events and their resilience to uncertainty will continue to be influenced by the ability of event organizers to make effective risk-based decisions under uncertain conditions within today's global risk society.

Cross-References

- ▶ Critical Infrastructure: Commercial Facilities Sector
- ▶ Emergency Management: Preparedness and Planning
- ▶ Event Security

References

Ash, J., & Smallman, C. (2010). A case study of decision making in emergencies. *Risk Management, 12*(3), 185–207.

Beck, U. (1992). *Risk society: Towards a new modernity.* London: Sage.

Beck, U. (2006). Living in the world risk society. *Economy and Society, 35*(3), 329–345.

Berlonghi, A. (1990). *The special event risk management manual*. Dayton: Bookmasters.

Blerter and ERMS. (2019). Event industry preparedness and resilience survey. Available from: https://www.blerter.com/lp/event-preparedness-resilience-survey-report?utm_campaign=2019%20IFEA%20Newsletter&utm_source=email&utm_medium=IFEA%20Newsletter. Accessed 12 Dec 2019.

Cambridge Dictionary. (no date) English Dictionary. Available at: https://dictionary.cambridge.org/dictionary/english/ (Accessed: 30 November 2019)

Elliot, D., Swartz, E., & Herbane, B. (2001). *Business continuity management: A crisis management approach* (2nd ed.). New York: Routledge.

Getz, D. (1997). *Event management and event tourism*. New York: Cognizant.

Goldblatt, J. (2011). *Special events: A new generation and the next frontier* (6th ed.). Hoboken: Wiley.

Hancock, B. (2019). A simpler way to assess risks?. Available at: https://erm.ncsu.edu/library/article/a-simpler-way-to-assess-risks. Accessed 15 Oct 2019.

Hillson, D. (ed) (2016) The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk. London: Kogan Page Ltd.

Hopkin, P. (2010). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (2nd ed.). London: Kogan Page.

International Organization for Standards. (2018). *ISO 31000: Risk management – Guidelines* (2nd ed.). Zurich: International Organization for Standards (ISO).

Khir, M. M. (2014). *Developing an event safety typology: A qualitative study of risk perception amongst event planners and venue managers in Malaysia.* Ph.D. thesis, Liverpool John Moores University. Available at: http://researchonline.ljmu.ac.uk/id/eprint/4441/1/157529_2014masrurphd.pdf. Accessed 9 Dec 2019.

Klein, G. (2008). Naturalistic decision making. *Human Factors, 50*(3), 456–460. Available from: https://journals-sagepub-com.ezproxy4.lib.le.ac.uk/doi/pdf/10.1518/001872008X288385. Accessed 3 Dec 2019.

Laybourn, P. (2003). Risk and decision making in events management. In I. Yeoman (Ed.), *Festival and events management: An international arts and culture perspective* (pp. 286–307). New York: Routledge. Available from: https://ebookcentral.proquest.com/lib/leicester/detail.action?docID=294126. Accessed 5 Nov 2019.

Lupton, D. (2013). *Risk* (2nd ed.). New York: Routledge.

McCaughey, G., Beckman, J., Schneider, G., & Down, K. (2017). Psychology of risk white paper: Old versus new – Embracing a new risk paradigm. Available from: https://www.acu.edu.au/-/media/whitepapers/psychology_of_risk_black_swan_white_paper_v2c.pdf?la=en&hash=9F697533273311D5A1277F16E7010A74. Accessed 3 Dec 2019.

Ostrom, L., & Wilhelmsen, C. (2012). *Risk assessment: Tools, techniques and their application* (1st ed.). New York: Wiley.

Piekarz, M., Jenkins, I., & Mills, P. (2015). *Risk and safety management in the leisure, events, tourism and sports industries*. Oxfordshire: CAB International.

Plous, S. (1993). *The psychology of judgement and decision making*. New York: McGraw-Hill.

Reason, J. (1997). *Managing the risks of organizational accidents*. Surrey: Ashgate Publishing.

Robson, L. (2009). *Perceptions of risk at meetings and conferences: An event planners perspective.* Ph.D. thesis, University of Waterloo. Available at: https://uwspace.uwaterloo.ca/bitstream/handle/10012/4509/Robson_Linda.pdf?sequence=1. Accessed 30 Nov 2019.

Rogers, G. (1997). The dynamics of risk perception: How does perceived risk respond to risk events? *Risk Analysis, 17*(6), 745–757.
Rutherford Silvers, J. (2008). *Risk management for meetings and events*. Oxford: Butterworth-Heinemann.
Slovic, P. (2000). *The perception of risk*. London: Earthscan Publications.
Talbot, J. (2011). What's right with risk matrices? 9 April 2011. Available at: https://www.juliantalbot.com/post/2018/07/31/whats-right-with-risk-matrices. Accessed 15 Nov 2019.
Talbot, J., & Jakeman, M. (2009). *Security risk management body of knowledge*. Hoboken: Wiley.
Tarlow, P. (2002). *Event risk management and safety*. New York: Wiley.
US Department of Homeland Security. (2011) Risk management fundamentals: Homeland security risk management doctrine. Washington, DC: US Department of Homeland Security.

Insider Threat

Adam D. Williams, Shannon N. Abbott and Adriane C. Littlefield
Center for Global Security and Cooperation, Sandia National Laboratories, Albuquerque, NM, USA

Keywords
Deception · Masqueraders · Traitors · Workplace crime

Definition

Insider threat refers to one or more individuals with authorized access to critical facilities, materials, or information who could attempt unauthorized removal or sabotage or who could aid in an external adversary to do so.

SAND2019-0545 J. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Introduction

While physical security is often perceived as guards, gates, and guns, all infrastructure security events have a human dimension. Any individual with authorized access to or knowledge of a site has the potential to play a role – positive or negative – in a security event. In most cases, this human dimension manifests in how personnel play a positive role in preventing, detecting, and responding to security events. In other cases, however, personnel play a negative role and facilitate security events through a lack of awareness, negligence, or unintentional acts. In extreme cases, individuals cause security events by committing *intentional* and *malicious* acts against critical facilities, materials, or information. These individuals could be *anyone*, to include those with regular (e.g., staff, management, janitorial, or security personnel), irregular (e.g., contractors, inspectors, or first responders), and limited (e.g., visitors or former employees) authorized access. This constitutes the so-called *insider threat*, a term defined by the National Insider Threat Task Force (2016) as:

> the risk [that] an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practices. (p. 3)

Thus, unlike external threats, the insider threat is difficult for organizations to address and mitigate because malicious insiders have "legitimate authorized access to your most confidential, valuable information systems, and they can use that legitimate access to perform criminal [or malicious] activity" (Cappelli et al. 2012, p. xviii). Although "many institutions have 'perimeter defenses' (gates, guards, access controls, and computer firewalls) [they] are nonetheless vulnerable to insider theft or destruction of critical data [materials, or facilities]" (NITTF 2016, p. 2). Most individuals will never attempt a malicious insider attack, but because any person with authorized access has the *potential* to do so, there is a need to adequately

address and mitigate the insider threat. This chapter will begin with a description of insider advantages, attributes, and motivations, as well as categories by which to evaluate potential insider threats. It will then outline broad concepts and strategies for preventing and mitigating insider threat attempts – to include steps to be taken *before* and *after* personnel are granted access, authority, and knowledge to critical pieces of infrastructure.

Insider Threat Advantages, Attributes, Motivations, and Categories

Unlike traditional, external threats that rely on overwhelming shows of force, the insider threat uses stealth (blending in to normal operations) or deceit (e.g., spoofing normal operations) to perpetrate a malicious act – leveraging key advantages of legitimate, authorized access to critical facilities, materials, or information. Authorized access to sensitive facilities or materials provides insiders with *time* to collect additional information or develop a plan for an attack. Potential insiders can use this time to operate at the margins of normal business practices (e.g., steal small quantities of materials below reporting thresholds), establish new behavioral patterns (e.g., regularly access a new vault), or change operational procedures (e.g., grant themselves network administration permissions) to avoid suspicion and detection. Additionally, insiders who wish to carry out a malicious attack have the *tools* necessary to do so – they know what capabilities the facility has (such as a crane to lift heavy items) and consequently do not have to bring in their own tools. For external attacks, a traditional concern for security designers is how many tools an adversary can bring into a facility. In contrast, an insider already has knowledge of and access to the necessary tools.

Time and access to tools lend insiders a third distinct advantage – the ability to *test* the system to identify whether an attack might be detected. Finally, insiders have the potential to leverage their position within the organization to influence the behavior of others. The influence of insiders can lead others to wittingly or unwittingly aid the insider with the attack (e.g., *teamwork*). Not all individuals who help insiders do so knowingly, as insiders can use their position to convince others to help in seemingly routine or benign ways. However, multiple insiders knowingly working together can be especially disastrous. The four advantages discussed above – time, tools, tests, and teamwork – increase the importance of addressing and mitigating the insider threat. Further, one way to describe insiders is in terms of four key attributes: access, authority, knowledge, and motivation.

Access includes the permission to be in a facility (or certain locations within a facility), to use specific materials or technology, and to view or obtain sensitive information. Typically, control over access is implemented to protect sensitive facilities, materials, and information. However, the primary distinguishing attribute of insiders is their permission to be in close proximity to or influence the use of sensitive facilities, materials, and information without setting off alarms or causing concern. Individuals with this level of access include all operational employees (such as staff and all levels of management) and support employees (such as the janitorial staff, security personnel, and other staff considered ancillary to a facility's primary objective). In addition, individuals with irregular access (such as inspectors, regulators, visitors, first responders, and maintenance personnel) can also pose a potential insider threat, as they have access to sensitive facilities, materials, or information that can be exploited in an insider attack. Consider, for example, "evidence of potential tampering as the cause of the abnormal condition" after engine coolant was found in the oil system of a diesel generator at the San Onofre Nuclear Power Plant in 2012 (Bunn and Sagan 2014, p. 1, footnote 2). This describes a potential insider scenario because not many individuals have permission to be near diesel generators at nuclear power plants, let alone to access the oil system without raising suspicion.

In addition to access, some insiders have *authority* or the power to influence behaviors or outcomes of people, procedures, or operations. Authority can be formal, to include hierarchical power structures (e.g., management and leadership

within an organization), control over communications protocols (e.g., supervising the central alarm station), and direct responsibility over sensitive operations. In addition, authority can be informal, to include influence driven by professional seniority or expertise, cultural norms, familial lineage, tribal affiliation, or personal affection. In addition to influencing people, authority can also influence operations – for example, an individual with authority could potentially delay the assessment and communication of an alarm to security personnel or ignore (and fail to report) patterns of unauthorized access of critical computer servers. Authority can even impact procedures, such as changing the protocols for retrieving items from a high security vault or making it more difficult to report anomalous security behaviors. Here, the £26.5 million heist from the Northern Bank case in Northern Ireland – in which one of the bank managers was convicted of an active role – is illustrative (Bunn and Sagan 2014).

Knowledge is an insider attribute that indicates a more detailed understanding of critical facilities, materials, or information than is held by the general public – and affords a potential insider additional benefits for carrying out an attack. First, insiders have knowledge of detailed facility layouts, operations, and normal business practices, while an outside attacker would know much less about a facility. Insider knowledge may include how to avoid or defeat protections at a facility such as security force capabilities and locations (or deployment strategies), details of security systems, or bypass activities for implemented protections. In addition, insider knowledge can include how to optimize targeting during an attack (e.g., to maximize damage to the facility or steal the most critical assets). Finally, insiders can combine all their knowledge to carry out an insider attack more expeditiously. Illustrating the role of knowledge in insider threat cases, one database demonstrated that "guards were responsible for 41 percent of insider thefts at non-nuclear guarded facilities" (Bunn and Sagan 2014, p. 4). For additional details, descriptions, examples, and case studies please see Hoffman et al. (1990) and Sagan and Bunn (2017) in the recommended readings list.

These attributes – authority, access, and knowledge – alone do not transform an average employee into an insider. Most often, this transformation is triggered by a *motivation* – or the reason(s) driving a set of actions or behaviors. There is no single motivation guaranteed to transition an individual with authority, access, and knowledge into a malicious insider, as different external or internal drivers motivate different individuals to act against sensitive facilities, materials, or information. For example, consider an individual with environmentalist sympathies who gains employment at an oil refinery in order to access and damage operational control rooms. This individual exhibits a *political* motivation, where the malicious act was used to raise awareness for a government or policy issue. Other common motivations include:

- *Ideological*: acting in response to a system of ideas and ideals, especially political beliefs.
- *Financial:* wanting or needing additional money.
- *Personal/disgruntlement:* an individual response to a perceived slight.
- *Psychotic*: mental instability driving behaviors.
- *Coercion*: external pressure applied to an individual, their family, or their assets to influence behavior (Homoliak et al. 2018; Tsenov et al. 2018).

Each distinct motivation may lead to insight for both the level of potential malicious intent and the likelihood the attempt will occur – and, therefore, helps identify appropriate mitigation strategies. For example, a disgruntled employee with a personal motivation is most likely to commit an insider attack in the 60 days before or after they are fired. This means facilities should more diligently monitor physical and cyber security in the days following an employee dismissal (e.g., cross-check access and change logs) (Collins et al. 2016). Ultimately not all insiders will attempt or carry out a malicious attack, but when insider opportunity is combined with insider motivations, an insider attempt becomes more likely.

Access, authority, knowledge, and motivation can be combined to define categories of potential insiders to understand the range of possible

malicious actions. Here, several questions help scope the range of insiders:

- Is the insider internally (e.g., disgruntlement) or externally (e.g., coercion) motivated toward malicious acts?
- What level of actions or involvement is the insider willing to commit in support of the malicious act?
- How violent is the insider willing to be in support of the malicious act?

The answers to these questions describe different roles insiders may take during a malicious act against sensitive facilities, materials, or information. If an insider is non-violent and does not actively participate in the malicious act, they are categorized as a *passive insider*. Passive insiders may intentionally (or unintentionally) pass information to an external adversary or may unintentionally aid in a malicious act (e.g., leaving a computer workstation unlocked) but will often stop if they believe they have been detected. These insiders may be looking to make extra money or could be coerced by an adversary who is blackmailing them in exchange for information. If an insider is non-violent but willing to contribute more actively to a malicious act, they are categorized as a *non-violent, active insider*. Active, non-violent insiders may leave doors unlocked, turn off security cameras, or grant unauthorized access to a computer network. Typically, active, non-violent insiders work with external adversaries (or other insiders) to achieve malicious aims, but they do not conduct the act themselves. If an insider is violent and willing to contribute even more actively to a malicious act, they can be categorized as a *violent, active insider*. Active, violent insiders likely execute the malicious act themselves – either with or without external help. Active, violent insiders are willing to inflict bodily harm on others in the facility and could have multiple motivations for the malicious act. These three categories help explain the insider threat and help identify best practices for detection, prevention, protection, and mitigation.

Many insiders have the access, authority, and knowledge to carry out an attack, giving them an *insider opportunity*. Yet, potential insiders also need a driver (or trigger event) to initiate an insider attack, requiring *insider motivations*. This suggests that an *insider attack* results from the combination of an *insider opportunity* (a function of access, authority, knowledge) and *insider motivations* (a function of internal or external drivers toward a malicious act).

Preventative Measures Against Insider Threats

While it is impossible to eliminate the insider threat, one method for identifying how to appropriately respond is evaluating individuals along a spectrum of access, authority, and knowledge. From this perspective, there are three states in which an insider can exist (Cappelli et al. 2012; Homoliak et al. 2018): (1) those applying for authorized access (e.g., job applicants or visitors); (2) those with authorized access – and presumably knowledge (e.g., employees, contractors, visitors); and (3) trusted individuals with additional opportunities (e.g., increased access permissions, management). People in each of these three categories have varying levels of access, authority, and knowledge which require different responses and technological, procedural, and administrative controls.

Preventative measures are mitigations aimed to prevent insider threat opportunities before they occur. More specifically, the goals of preventative measures are to exclude potential insiders by identifying undesirable behavior or characteristics *before* allowing access and to minimize opportunities for malicious acts by limiting access, authority, and knowledge. Preventative measures can take place before individuals are granted access, such as during the hiring process for employees, or through a set of procedures laid out for irregular access, like visits from first responders. However, preventative measures can also take place after access has been granted – though post-access preventative measures are more difficult to implement. The two most successful and well-known preventative strategies include trustworthiness programs and promoting strong security culture.

Trustworthiness programs have no official or common definition, but a working definition would include all efforts, initiatives, and processes to ensure that employees are vetted and found to be responsible, upstanding, and principled. Key elements of trustworthiness programs include a threat or risk assessment, well-defined personnel security requirements, effective implementation of the program, and regular review and evaluation of effectiveness. Delving further into these key elements, a threat or risk assessment should consider potential adversaries including their intent, capabilities, and tactics, understand potential targets at each facility, and understand possible insider motivations. The risk assessment should be used to scale the trustworthiness program to the risk at a given facility and inform personnel security requirements. The second key element, personnel security requirements, should define information and physical access levels, set eligibility criteria for access, and be codified through legal or regulatory mechanisms. Third, trustworthiness program implementation should establish standardized personnel screening processes that could include pre-employment background checks, psychological or medical evaluations, adjudication mechanisms for handling disputes, and continued reinvestigation. Finally, trustworthiness programs should be regularly reviewed and evaluated and anomalous activities and incidents should be thoroughly investigated and reported. Examples of trustworthiness programs include the Human Reliability Program (US DOE), Access Authorization Programs (US NRC), and Personnel Security Programs (implemented internationally).

Unlike trustworthiness programs, which aim to determine if a person should be allowed access, the goal of security culture is to promote and reinforce good security practices while individuals have access to the facility. The concept of security culture ultimately stems from the broader theory of organizational culture, which argues that the dynamics of organizations can be described by the interactions between core beliefs (e.g., underlying assumptions), shared characteristics (e.g., espoused values), and observable behaviors (e.g., visible artifacts) (Schein 1990). In the nuclear security context, this emphasis shifts to perception of the existence of a credible threat and the belief that nuclear security is vital to combatting such threats. However, Cole et al. (2013) offer a review by human factor experts at Sandia National Laboratories that identified a range of interpretations for the term safety culture. While safety culture and security culture have different end goals, they face similar challenges in their implementation. To be successful in improving security culture, organizations should promote values such as awareness, reporting, flexibility, learning, and just practices.

In order for security culture to take hold there must be buy-in from senior leadership and management. While security culture can be influenced by the international community, national regulations and priorities, public support, norms, and threat credibility, it is ultimately manifested in management systems and employee behaviors. A badging system only works well when everyone has to wear a badge – including the president of the organization. Insider prevention is only as good as the security and security culture of an organization.

Protective Measures to Mitigate Insider Threats

Where preventative measures seek to ensure that a threat does not access a facility, *protective measures* initialize when preventative measures have failed – meaning that potential insiders have been granted authorized access. Protective measures are implemented to inhibit inappropriate access to sensitive facilities, materials, or information by those with authorized access to a subset of these assets. Similar to the objectives of physical security, the goals of protective measures are to detect, delay, and respond to malicious insider acts to mitigate or minimize negative consequences. Protective measures take place after individuals are granted regular access (e.g., after being hired), enhanced access (e.g., additional clearances are granted), and irregular access (e.g., once inspectors or visitors are on the premises). Two common protective strategies include

access control systems and employees reporting suspicious behavior.

Access control technologies are implemented to intentionally restrict proximity to (or contact with) sensitive facilities, materials, or information. In so doing, the protective measure distinguishes between who does (and who does not) have authorized access – a direct protection against potential insider threats. For example, access to a nuclear power plant's control room can range from visitors being escorted on tours to operators entering the room unescorted during business hours to power plant management with the authority to enter the control room during nonbusiness hours. In addition, access controls protect against the insider threat by helping facilities systematize and expedite decisions regarding who can appropriately access what locations, materials, or information with their facility. Access control technologies can include badge readers, biometrics, passwords, physical locks, pin code-based controls, or some combination of these technologies to ensure only trusted employees can access sensitive locations, information, and materials. Access control technologies, then, actively restrict – and account for – all individuals attempting to access sensitive assets to protect them against potential malicious insider acts.

While access control technologies provide enhanced protection against the insider threat, they are only effective if the databases and supporting digital infrastructure are themselves protected. If an insider can edit the access control database, they can allow themselves or others authorized access to any facility or location within it. Yet, protections on these databases and networks work in concert with traditional access controls in reinforcing dynamics to improve insider threat protection. There is a similarly high need for vigilance in individuals with access control responsibilities (including managing the related databases) to protect against insiders. Individual vigilance can be supported by organizational procedures (e.g., implementing the two-person rule for access or strict change management procedures) and improving security culture. Additionally, if an insider successfully executes a malicious act, access controls can be used forensically to support attribution of the malicious act. For example, badge reader data for a toxic chemical storage vault can help identify a disgruntled maintenance worker who poured a hazardous liquid into the facility's ventilation system.

As potential insiders know many of the technological protections in place, a second protective measure relates to employee observation of behavioral patterns to limit the ability for unauthorized access. Behavioral reporting programs are related to preventive measures (e.g., human reliability programs and nuclear security culture) but include more formalized protocols to stop the inappropriate access of sensitive facilities, materials, and information by individuals with authorized access. Like their technological counterparts, protective measures based on behavioral observations can become more stringent based on the sensitivity of facilities, materials, or information. For example, concerning political statements made by janitorial staff should not warrant the same level of potential concern as those same comments made by a chief scientific officer with unfettered facility access. In general, reporting of unusual or suspicious behavior should not lead immediately to disciplinary action, but rather to a comprehensive investigation to determine if an insider may have developed the motivation to carry out an attack.

In addition to requiring high-level support, organizations must consider behavioral reporting programs carefully. One major challenge behavioral reporting programs face is the potential conflict with social culture or personal feelings, where employees are reluctant to "betray" a friend/colleague or feel betrayed by those who reported them. Thus, success of these types of protective measures is based on employees feeling comfortable about reporting suspicious or unusual behaviors of their colleagues without fear of reprisal. In order to avoid some of the negative feelings that can arise from behavioral reporting programs, companies must have a clear definition of what "suspicious behaviors" are and when they expect their employees to report. Unclear definitions and guidelines can cause confusion and lead to frustration and anger. Finally, organizations must have timely and "fair" responses to indicators and behavioral reports – along with robust records to document the justification for their decisions. Example of "fair" responses to reports of

suspicious or unusual behaviors typically ranges from intensified monitoring to restrictions in job responsibilities to termination and even legal action.

Conclusion

Sustaining a high-performing insider threat mitigation strategy is challenged by the difficulty in achieving – and maintaining – high levels of human reliability surrounding sensitive facilities, materials, and information. One difficulty in human reliability is the conflict between high-quality insider threat initiatives (e.g., enhanced performance monitoring), legal/regulatory requirements, and individual privacy. Another difficulty is often posed by the underlying social culture, especially if cultural sensitivities tend toward a lack of trust in government (or non-familial authority), high levels of tribal loyalty, or an inherent trust of others. In addition, it is difficult to measure the effectiveness of insider threat mitigation programs, as proving that an insider attack did not happen *because* of a robust insider threat program is extremely challenging. Despite this, evidence suggests these programs have been successful in mitigating insider threats. To this end, Bunn and Sagan (2014) present ten lessons learned from past insider threat cases and declare the "main lesson of all these cases is: do not assume, always assess – and asses (and test) as realistically as possible" (p. 20).

The potential for insider threats poses an evolving, multifaceted set of challenges to the security of sensitive facilities, materials, or information. As discussed above, potential mitigation strategies must be similarly flexible, wide-ranging, and applied continuously throughout the period that individuals have (or are seeking) authorized access to sensitive assets. In response, the US National Insider Threat Task Force has published a set of best practices to help outline appropriate insider threat mitigation strategies (2016, 2017). These best practices include decide who should be engaged, determine what matters most to your organization, reassess personnel management practices, develop clear termination procedures, engage the workforce, review systems for security/vulnerability, engage your privacy experts, put information in context, and test your security posture. In addition to regular testing, insider threat mitigation strategies should be updated each time a significant challenge is identified. The need for vigilance and diligence in insider threat mitigation stresses "a dynamic effort requiring constant evaluation, fresh perspectives, and updated approaches" (NITTF 2017) to effectively detect, prevent, mitigate, and protect against insider threats.

Cross-References

- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
- ▶ Physical Security: Best Practices
- ▶ Security Management

References

Bunn, M., & Sagan, S. (2014). *A worst practices guide to insider threats: Lessons from past mistakes*. Cambridge, MA: American Academy of Arts & Sciences.

Cole, K. S., Stevens-Adams, S. M., & Wenner, C. A. (2013). *A literature review of safety culture (SAND2013-2754)*. Albuquerque: Sandia National Laboratories.

Collins, M. L., Theis, M. C., Trzeciak, R. F., Strozer, J. R., Clark, J. W., Costa, D. L., Cassidy, T., Albrethsen, M. J., & Moore, A. P. (2016). *Common sense guide to mitigating insider threats* (CMU/SEI-2016-TR-015, CERT Insider Threat Center) (5th ed.). Pittsburgh: Carnegie Mellon University.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M. (2018). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys, preprint- arXiv: 1805.01612*

National Insider Threat Task Force. (2016). *Protect your organization from the inside out: Government best practices*. Washington, DC: Government Printing Office.

National Insider Threat Task Force. (2017). *Insider threat guide: A compendium of best practices to accompany the National Insider Threat Minimum Standards*. Washington, DC: Government Printing Office.

Schein, E. (1990). Organizational culture. *American Psychologist, 45*(2), 109–119.

Tsenov, B. G., Emery, R. J., Whitehead, L. W., Reingle Gonzalez, J., & Gemeinhardt, G. L. (2018). A pilot examination of the methods used to counteract insider threat security risks associated with the use of radioactive materials in the research and clinical setting. *Health Physics, 114*(3), 352–359.

Further Reading

Bunn, M., & Sagan, S. (Eds.). (2017). *Insider threats*. Ithaca: Cornell University Press.

Cappelli, D., Moore, A., & Trzeciak, T. (2012). *The CERT® guide to insider threats: How to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud)*. Upper Saddle River: Addison-Wesley.

Hoffman, B., Meyer, C., Schwarz, B., & Duncan, J. (1990). *Insider crime: The threat the nuclear facilities and programs*. Santa Monica: RAND.

Intelligence

Keith Cozine
College of Professional Studies, St. John's University, Queens, New York City, NY, USA

Keywords

Intelligence Community · Collection Disciplines · Intelligence Cycle

Definition

Intelligence is information that has been collected, processed, analyzed, and disseminated to policy and decision-makers at their direction to fulfilling their needs and provide knowledge or foreknowledge of issues of concern.

Introduction

When people hear the word intelligence in terms of national or homeland security, they often think that it is "nothing more than information that is secret, or relate it to covert action or espionage depicted in movies whose main characters are named James Bond or Jason Bourne" (Cozine 2015, p. 81). The reality is, especially in a post-September 11th world, intelligence is much more than secret information and spying, and what is seen in the movies and television is often far from reality. In fact, James Bond and Jason Bourne would make terrible intelligence officers because a successful intelligence officer is discreet and would not drive fancy sports cars while wearing a tuxedo or engage in hand to hand combat in a crowded market place (Cozine 2015). In the United States, while the Central Intelligence Agency (CIA) or the National Security Agency (NSA) are what that pop into people mind, but there are actually a number of other agencies that are part of the nation's Intelligence Community (IC), but there are actually a number of other agencies that are part of the nation's Intelligence Community (IC), as well as a host of federal agencies outside of the IC, state and local agencies, and increasingly the private sector that play a role as both "consumers" and "producers" of intelligence. Likewise, the sources of intelligence are not just spying on our adversaries but rather from various collection disciplines, each with their own unique sources and methods for gathering information. Given these common misconceptions about intelligence, the next section seeks to shed light on what intelligence really is.

What Is Intelligence?

According to Lowenthal (2020), a great deal of people think that intelligence is nothing more than information that is secret. However, "information is anything that can be known, regardless of how it was discovered." Intelligence, on the other hand, is information that meets the need of policy or decision-makers that has been collected, processed, and narrowed to meet those needs (Lowenthal 2020, p. 1) Intelligence, when it is disseminated, is often referred to as a "product" and those who it is produced for are "consumers" (FAS 1995). Just like any other commercial product that fills the needs or meets a market's demand, an intelligence product must also meet the demands of the consumer; thus, intelligence is consumer driven. Consumers anticipate that they will need information or have a question answered before planning a task or making a decision and they will charge an intelligence organization with providing the information or answering the question. This tasking is known as an intelligence requirement. It is then up to the intelligence organization to meet the needs of the consumer and fulfill the intelligence requirement. However,

intelligence is not about truth or a definitive answer as the analyst will almost never have the complete picture. The goal is to produce a product that is reliable, unbiased, and honest (Lowenthal 2020).

Intelligence allows its consumers, ranging from high-level policy-makers to frontline personnel to make decisions, take action, consider possible alternatives, and predict possible outcomes. Intelligence can consist of both classified and unclassified information (Lowenthal 2020). As Lowenthal (2020) stated, "[a]ll intelligence is information. . .[but] not all information is intelligence" (p. 1). Intelligence can be categorized as strategic, anticipatory (often referred to as tactical), and operational. Strategic intelligence "identifies and assesses the capabilities, activities, and intentions of states and non-state entities to develop a deep understanding of the strategic environment, warn of future developments on issues of enduring interest, and support U.S. national security policy and strategy decisions" (ODNI 2019b, p. 8) Anticipatory intelligence identifies and assesses "new, emerging trends, changing conditions, and underappreciated developments to challenge long-standing assumptions, encourage new perspectives, identify new opportunities, and provide warning of threats to U.S. interests" (ODNI 2019b, p. 9). The goal of current operational intelligence is to provide "timely intelligence support to enable planned and ongoing operations" (ODNI 2019b, p.10). Like war, intelligence has a long history, not just within the United States but around the world.

History of US Intelligence

Intelligence within the United States traces its roots back to the Revolutionary War. As the commander-in-chief of the Continental Army during the war, General George Washington knew how important intelligence was to the Continental Army and its ability to win the war. Intelligence was vital to the effort to defeat a more powerful, better-funded, and better-organized British army, the world's reigning superpower at the time. General Washington and the Continental Army "ran networks of agents and double agents; set up elaborate deceptions against the British army; coordinated sabotage operations and paramilitary raids; used codes and ciphers; and disseminated propaganda and disinformation to influence foreign governments" (Central Intelligence Agency 2007a). They even uncovered a traitor within their own ranks, the infamous Benedict Arnold. In the very first presidential State of the Union address, the now president of Washington requested that Congress establish a "secret service fund" for clandestine activities. "Under Washington's Presidency[,] intelligence spending was higher than at any time in the country's history amounting to 12 % of the national budget" (Central Intelligence Agency 2007a).

The importance placed on intelligence on a national level did not last much beyond the Washington Presidency. The reason is, especially after the War of 1812, the United States did not have a strong foreign policy interest beyond its borders. Up until World War II, intelligence operations, capacities, and organizations were piecemealed together as the United States found itself involved in conflicts at home and abroad. In fact, during the period between the War of 1812 and World War II, the United States had only one continuous intelligence organization, the Office of Naval Intelligence, which was established in1882 and remains the oldest intelligence organization in the nation. Overall, intelligence was seen as a law enforcement function focusing on domestic concerns, such as criminal enterprises, and preventing foreign intelligence operations and influence. The United States' ability to collect foreign intelligence eroded and it wasn't until Congress declared war on Germany in 1917 that the military received more resources to increase its intelligence capability. After the War, US abilities to collect foreign intelligence and conduct covert actions were greatly diminished as intelligence entities' budgets were substantially reduced (Central Intelligence Agency 2007a). This diminishing of the United States' intelligence capabilities all changed in the lead up to World War II. In 1941, when it seemed inevitable that the United States was going to end up involved in the conflict that President Roosevelt established the first

peacetime, independent intelligence agency, the Office of the Coordinator of Information. The Office of the Coordinator of Information was designed only to organize the activities of several agencies' intelligence functions, but the lack of intelligence that could have prevented the attack on Pearl Harbor shed light on the faults with this approach of simply coordinating intelligence activities. As a result, a larger and more diversified agency, the Office of Strategic Services (OSS), was established in 1942 to succeed the Coordinator of Information. The OSS is the forerunner of today's Central Intelligence Agency (2007a).

Following the War, as was the case throughout the nation's history, there was sentiment for the need to return to the normalcy of the pre-war military positioning and demobilization began. This included the abolishing of the OSS in October 1945 as the nation's only civilian intelligence agency. This demobilization did not last however, as the perceived threat of the Soviet Union and the looming Cold War, illustrated the the need for a centralized intelligence system, even in peacetime was recognized. In 1947, President Truman signed into law the National Security Act of 1947, representing the largest government reorganization in US history and establishing national security framework for the next half century. Among other things, the Act established Central Intelligence Agency (CIA) as an independent civilian intelligence organization with the Director of Central Intelligence as its head while also serving as head of the Intelligence Community and principal intelligence advisor to the National Security Council and the President. The CIA was charged with "coordinating the nation's intelligence activities and correlating, evaluating, and disseminating intelligence that affects national security," while also expressly prohibiting the CIA from having any "police, subpoena, law-enforcement powers, or internal security functions" (Central Intelligence Agency 2007b). Over the next 50 years, other intelligence organizations were established to provide for greater intelligence coverage leveraging new advancements in technology or emerging issues.

Traditionally, intelligence is thought of as a national security issue relating to defense and foreign policy. In the aftermath of the September 11th attacks, there was a realization that the threats and dangers the United States faced were not only from hostile nation-states but also from dangerous non-state actors, such as terrorist groups and transnational organized crime. As a result, there has been an increased emphasis placed on homeland or internal security, including the realization that local and state agencies mostly play a greater role in the nation's intelligence apparatus. The attacks were also perceived as a major intelligence failure. To address this intelligence failure, President George W. Bush signed into law, among other laws, the Intelligence Reform and Terrorism Prevention Act of 2004. Like the National Security Act of 1947, this Act represented a major overhaul of the nation's intelligence system. The Act established the cabinet-level position of the Director of National Intelligence, tasked with managing the National Intelligence Program (NIP), and replaced the DCI and the head of the IC. The Act also established and defined the concept of national intelligence which "includes information gathered in the United States or abroad that pertains to more than one agency and involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on national or homeland security" (S. 2845 2004) National intelligence, therefore, bridges the foreign-domestic divide, includes a focus on homeland security as well as the traditional IC focus on foreign intelligence, and identifies the need for knowledge sharing among IC agencies in order to be utilized effectively. To create national intelligence for a diverse set of consumers, information needs to be collected, processed, analyzed, and narrowed to meet the specific needs of decision- and policy-makers.

Intelligence Collection

Intelligence collection is not new and the various ways that intelligence has been collected have developed over time. Its advancements in technology have ultimately led to new approaches for

intelligence to be collected leading to the development of five distinct principal methods to collect intelligence (i.e., collection disciplines). These collection disciplines are as follows:

1. Human-Source Intelligence (HUMINT). HUMINT refers to intelligence obtained from human sources and includes overt, clandestine, or covert activities and those individuals who exploit, manage, or support these activities. Overt HUMINT sources can include attaches and diplomatic personnel, official delegations, debriefing of refugees, and inmates in detention centers and prisons. Clandestine HUMINT sources are primarily agents who have been recruited by a case officer from an intelligence organization or have volunteered to provide information or infiltrate an organization to gather information or intelligence about a particular target (Cozine 2017). A Covert HUMINT source is one where the relationship between the agent and the sponsor will never be acknowledged. In these cases, the covert source will generally leave the country under the guise of being political refugees or need to be exfiltrated from the country (Althoff 2015).
2. Signals Intelligence (SIGINT). "*SIGINT* is derived from signal intercepts comprising – however transmitted – either individually or in combination: all communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT)" (ODNI 2019b). COMINT "includes information derived from intercepted communications transmissions. . . [and] targets "voice and teleprinter traffic, video, Morse code traffic, or even facsimile messages" (Nolte 2015, p. 81), while ELINT covers non-communications transmissions, such as radar that are intercepted and analyzed. FISINT, on the other hand, consists of "intercepts of telemetry from an opponent's weapons systems as they are being tested. Telemetry units provide designers with information on a prototype's guidance system operation, fuel usage, staging, and other parameters vital for understanding operational characteristics" (Nolte 2015, p. 98). SIGINT's roots can be traced back to World War I when the British successfully began intercepting German communications by tapping underwater cables. Today, it is collected by a variety of Earth-based methods, such as ships, planes, and ground sites or from space by satellites. An advantage of SIGINT is that it provides insight into what is being said, planned, or considered by reading messages and determining meaning through content analysis. A disadvantage of SIGINT is that targets of collection efforts can use encryption devices in order to conceal the content of their communications or can use false transmissions to conceal their true intentions (Lowenthal 2020).
3. Geospatial Intelligence (GEOINT). GEOINT refers to "the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information" (National System for Geospatial Intelligence 2018, p. 3). Geospatial information can be more readily defined as "data, information, and knowledge gathered about entities that can be referenced to a particular location on, above, or below the earth's surface" (Murdock and Clark 2015, p. 111). GEOINT combines an image with intelligence and geospatial information about the location of the image to try to determine what the image means in terms of a specific intelligence requirement. Imagery is usually in the form of photographs, but it can also include other types of images such as infrared imagery or spectral analysis that measures changes in the reflections of certain rays of light within the spectrum. One of the big advantages of GEOINT is that it is easy to understand and interpret. A major disadvantage is it is only a snapshot or a photograph of a particular place at a particular time and that it is susceptible to denial and deception techniques, such as using camouflage or the avoidance of engaging in illicit activities during satellite passes (Lowenthal 2020).

4. Measurement and Signature Intelligence (MASINT). MASINT is "scientific and technical intelligence information obtained by quantitative and qualitative analysis of data" that "enables detection, location, tracking, identification and description of the unique characteristic of fixed and dynamic target sources". It employs "a broad group of disciplines including nuclear, optical, radio frequency, acoustics, seismic, and materials sciences" (ODNI 2019b). MASINT is used to identify gases or waste leaving factories or other facilities, indications of nuclear development, and other specific characteristics or materials related to the development of weapons systems and the development of WMDs by both state and non-state actors. MASINT has six distinct sub-disciplines: (a) electro-optical, which measures the properties emitted or reflected from the various types of light including both visible and non-visible light; (b) geophysical, which measures disturbances and anomalies on physical fields on the surface of the Earth, such as acoustics, gravity, and magnetic and seismic activities; (c) material, which measures the composition and identifies various gases, liquids, and solids; (d) nuclear, that measures the quantities and qualities of nuclear signature, such as gamma rays, X-rays, and neutrons; (e) radar, which measures the properties of radio waves reflected from targets or objects; (f) and radio frequency, which measures the electromagnetic signals generated by an object and its various band widths (Morris and Clark 2015). One of MASINT's biggest advantages is that it is difficult for collection targets to implement denial and deception countermeasures because of the scientific nature of the discipline. For example, it would be difficult to conceal or alter the heat signature of certain types of weapons. However, the scientific and technical nature is sometimes a disadvantage too as MASINT is not appreciated or easily understood by some intelligence consumers, especially policy-makers (Lowenthal 2020).
5. Open-Source Intelligence (OSINT). OSINT is "publicly available information appearing in print or electronic form including radio, television, newspapers, journals, the Internet, commercial databases, and videos, graphics, and drawings" (ODNI 2019b). OSINT is defined by the National Defense Authorization Act of 2006 as "information that is publicly available to any one through legal means, including request, observation or purchase, that is subsequently acquired, vetted and analyzed, in order to fulfill an intelligence requirement" (Jardine 2015, p. 6). Publicly available means the information is available to any member of the general public. Available information is not necessarily free; it could be accessed and/or obtained with purchase. It cannot be obtained through any act of trespassing, theft, hacking, or use of social engineering, all of which would be illegal, and it also means that it cannot be considered publicly available. It must be vetted and analyzed to appraise, verify, or check for accuracy, authenticity, and validity. Finally, it must fulfill an intelligence requirement of a consumer (Jardine 2015). The advantage of OSINT is that it is readily available and is an excellent starting point for all other collection efforts. OSINT can assist framing a problem, quickly establish what is known through open sources, where intelligence gaps exist, and where other INTs must try and fill in the missing pieces. The major disadvantages include (but are not limited to) the following: sheer amount of data is available from open sources, reliability of sources is unknown, and public data may be intentionally manipulated or taken out of contexts (Lowenthal 2020).

The Intelligence Cycle

As stated earlier, intelligence is much more than simply collecting information or data. Intelligence is an entire process used to create a finished intelligence product to meet the specific needs of policy-makers. The process by which this is achieved is known as the intelligence cycle, a five-step process made up of planning and direction, collection, processing, analysis and production, and dissemination. The process is called a cycle

because it is circular in nature. An intelligence product may lead to new questions and the need for new intelligence. The process can become never-ending progression of developing intelligence for as long as consumers needs for intelligence on a specific topic exist. There are checks and balances at each stage of the process that must be completed before moving on to the next step in order to ensure that reliable and accurate intelligence is created. While this view sometimes oversimplifies what actually occurs, it is a useful construct for understanding the basic functions that any intelligence enterprise must accomplish to be successful.

The first step of the intelligence cycle is planning and direction, which begins when policymakers or other decision-makers express a need for intelligence information. This need for intelligence information is referred to as an intelligence requirement. This requirement is passed to an intelligence agency, where an answer is developed and then disseminated to thee requesting policymaker (Lowenthal 2020). Today's threat environment represents an endless and complex array of information, making it infeasible for intelligence agencies with limited resources to cover every possible threat with equal attention. As a result, some issues and targets will receive top priority; others will only receive peripheral attention, while still others will receive little if any notice. The challenge is setting requirements that dictate which issues or targets receive highest priority. In short, it is about establishing what issues are of greatest importance and what data must be collected and analyzed to provide the best possible answers. Within the US intelligence framework at the federal level, it is "policy-makers, including the president, his or her advisers, the National Security Council, and other major departments and agencies of government, initiate requests for intelligence" (ODNI 2019b). The issue coordinators within the IC interact with these policy-makers to identify core concerns and requirements. It is the formulation, establishment, and evaluation of these intelligence requirements that is an important element of starting the intelligence cycle and pointing it in the right direction. If priorities and resources are misallocated, chances are greater that collectors will overlook important information that cannot then contribute to subsequent stages of the intelligence process (Lahneman 2017).

The next step of the process is collection. In response to the established intelligence requirements, an intelligence agency develops an intelligence collection plan. This plan evaluates available sources and methods already available within their own organization and may also seek intelligence from other agencies. After this existing intelligence is considered, a determination is made to see what additional information or data need to be collected to fulfill that requirement. These additional needs are usually referred to as a collection requirement (ODNI 2019b). To fulfill collection requirements, decisions have to be made on how to acquire the required information, what assets are in place to collect it, where to collect it, when to collect it, and then physically acquiring the information. As discussed in the previous section, depending on the agency and its capabilities, sources may include HUMINT, GEOINT, MASINT, SIGINT, and OSINT. These methods of collection share one major commonality: they are all resource intensive. Launching satellites, intercepting signals, and running agent networks are all costly. Accordingly, managers of the different collection disciplines compete for limited budgetary resources (Lowenthal 2020). The information that is acquired during the collection phase and forwarded on to the next step of the cycle is known as raw intelligence.

Collection systems accumulate vast quantities of information, of which only a fraction is usable. Not only must the relevant information be identified and separated, but it must also be repackaged in accessible ways. This need to repackage the data gives rise to the processing and exploitation phase of the intelligence cycle. This phase is where raw data is turned into a form usable for analysis. Skilled specialists must sift through collected information in search of useful intelligence. The techniques used in filtering information include "exploiting imagery, decoding messages and translating broadcasts, reducing telemetry to meaningful measures, preparing information for computer processing, storage and retrieval,

placing human-source reports into a form and context to make them more understandable" (ODNI 2019b). For example, photo-satellites capture thousands of images across the planet, all varying in terms of resolution, angles, daylight, and weather conditions. To the untrained eye, all these variations could mean nothing, but professionals who have expertise in imagery are able to screen each image for subtle clues and indicators that might suggest an important finding. Similarly, other intelligence professionals such as code breakers, translators, and weapons experts use their own expertise to sift out the most relevant information (Lahneman 2017). At the end of the processing and exploitation stage, raw intelligence is passed on to the next phase for analysis and production.

During the analysis and production stage, raw intelligence is integrated, evaluated, and analyzed for the preparation of intelligence products that seek to fulfill the intelligence requirements transmitted by the consumer. Analysis is considered to be the most important part of the intelligence cycle because it is where information is converted into finished intelligence. For this reason, analysts are often considered the most important persons within the intelligence cycle. Analysts are specially trained employees of intelligence organizations who typically combine substantive expertise in a variety of issues to "integrate data into a coherent whole, put the evaluated information in context, and produce finished intelligence that includes assessments of events and judgments about the implications" (FAS 1995). Analysts rely on their keen analytic capacities and strong written and oral communication skills to achieve this function successfully. In short, their job is to assemble many different pieces of collected and processed information, evaluate this information in terms of their specialized knowledge, consider its implications for security and policy interests, and succinctly disseminate these judgments in written and oral formats as appropriate.

Dissemination, the last stage of the intelligence cycle, refers to the distribution of intelligence products to the policy-makers who requested them. After information is collected, combined with data from other possible sources, organized, and analyzed to create finished intelligence, it can be disseminated directly to the same policy-makers whose initial needs generated the intelligence requirements. Dissemination is all about getting the right intelligence to the right people at the right time. It is a rigorous job that represents the sum efforts of all previous stages combined. The Office of the Director of National Intelligence (2019b) identifies five categories of finished intelligence:

> "current intelligence, that addresses day-to-day events; estimative intelligence, that looks forward to assess potential developments that could affect U.S. national security: warning intelligence, that sounds an alarm or gives notice to policy-makers; scientific and technical intelligence, that includes an examination of the technical development, characteristics, performance and capabilities of foreign technologies, including weapon systems or subsystems; research intelligence, that supports other finished intelligence products (p. 7)."

Most intelligence consumers are inundated with a constant barrage of competing information and intelligence reports. These reports may constitute only a fraction of the documents they receive. As a result, intelligence professionals must find ways to customize reports for different types of consumers and put them together in ways that convey the most important information in the least demanding fashion (Lahneman 2017).

While dissemination of finished intelligence represents the last step of the intelligence cycle, it does not represent the end of the intelligence process. Despite the best collection and analytical efforts, intelligence does not exist until consumers acknowledge it, understand it, and then make decisions based on this intelligence. When an intelligence product is disseminated, it is often taken for granted that policy-makers will digest and act upon the intelligence they receive, but this outcome is by no means guaranteed. When the consumer does review and hopefully use finished intelligence, they will often provide feedback to the intelligence producers. Feedback is when consumers evaluate the intelligence organization's performance on any of the parts of the intelligence cycle and provide recommendations for future improvement. Additionally, after intelligence is disseminated, the consumer may provide

feedback in the form of more questions to be answered or a request for more information. These requests results in the creation of new direction and intelligence requirements being established. These new requirements return to the planning and direction stage starting the cycle over again.

Who Creates Intelligence?

The intelligence process refers to the process of how intelligence is created, but who is responsible for producing it. At the federal level, it is the intelligence community that serves as the primary intelligence apparatus of the nation. As mentioned earlier in this chapter, the National Security Act of 1947 laid the foundation of the United States' modern security infrastructure, and in doing so, it structured a cooperative framework known as the intelligence community (IC). The goal of the IC is to unite and coordinate the formerly disparate intelligence agencies. The core mission of the IC has remained to "work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States" (Office of Naval Intelligence n.d.). Currently, the IC is composed of seventeen separate agencies. The IC draws its membership from five executive branch departments and one independent agency. These agencies perform a variety of intelligence and counterintelligence functions and report to different civilian and military clients. The IC is accountable to a Director of National Intelligence who tasked with overseeing the operations of the entire IC. The IC's current structure evolved piecemeal as a result of Cold War, developments and advances in technology, the intricacy of the intelligence process and the presence of many different intelligence consumers. It is these consumeers, with widely different requirements, that dictate the structure of the US national intelligence apparatus.

Eight out of the seventeen agencies of the US IC are located in the Department of Defense (DOD) and it administers an estimated 80% of the entire intelligence budget. Each agency has its own director that oversees its operation; they are all ultimately accountable to the Under Secretary of Defense for Intelligence, and through this official, to the Secretary of Defense (Lowenthal 2020). Within DOD, there are four agencies that are members of the IC: the National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), and the Defense Intelligence Agency (DIA).

The NSA has a three-pronged mission. First, it functions as the IC's primary collector of SIGINT. The SIGINT mission is to collect, process, and disseminate intelligence derived from foreign communication, electronic, and instrument signals for intelligence and counterintelligence purposes, as well as to support for military operations. Second, it is responsible for information assurance (IA) in which the NSA attempts to prevent foreign intelligence agencies and other adversaries from gaining access to sensitive or classified national security information and collecting intelligence. Third, is the Central Security Service (CSS) that provides cryptologic support to the intelligence community and military. The NGA provides GEOINT to a wide array of policy-makers, military commanders, and intelligence professionals, as well as first responders and others involved in disaster management. The NRO is in charge of designing, building, launching, and maintaining America's intelligence satellites. The DIA, established in 1961 to centralize the intelligence received by the service branch agencies, provides "military intelligence to warfighters, defense policy-makers and force planners in the Department of Defense and the Intelligence Community in support of U.S. military planning and operations, and weapon systems acquisition" (DIA n.d.). Each branch of the armed forces within DOD (Army, Navy, Air Force, and Marine Corps) maintains its own intelligence organization to support the mission effectiveness of its respective service.

In addition to those members of the IC that are within DOD, there are also seven IC members that are considered departmental intelligence organizations in that they are houses within a cabinet-level department and report to the head of that department who are their primary consumers. The State Department's Bureau of Intelligence

and Research's (INR) primary mission is to produce intelligence products to support US diplomat efforts by providing independent analysis of events to the state department policy-makers to support foreign policy and national security efforts within the department. The Department of Energy's (DOE) Office of Intelligence and Counterintelligence is responsible for protecting vital scientific and technological national security information and providing scientific and technological expertise in support of policy-makers. The Department of the Treasury's (DOT) Office of Intelligence and Analysis (OIA) mission is to deliver timely, accurate, and relevant intelligence to decision-makers to protect financial integrity of the country by assessing and identifying threats and vulnerabilities into the nation's financial infrastructure. There are two organizations that are within the Department of Justice (DOJ) that are members of the IC. The Federal Bureau of Investigation (FBI) not only serves as an investigative law enforcement agency but also collects and produces intelligence to support its own investigations and creates products that support partner agencies and help those agencies to better understand and face the security threats the nation faces domestically. Likewise, the Drug Enforcement Administration (DEA) has a dual law enforcement and intelligence responsibility. The DEA's Intelligence Program initiates new investigations into violations of controlled substance laws and major drug organizations, support ongoing investigations, and provide policy-makers with intelligence products related to drug trend information. Like DOJ, the Department of Homeland Security (DHS) also has two components that are members of the IC. DHS's Office of Intelligence and Analysis (I&A) mandate is to equip its federal, state, and local partners as well as certain components of the private sector with the timely intelligence and information to assist them in keeping the homeland safe and secure. I&A serves as a conduit between the IC and the Homeland Security Enterprise to deliver intelligence to enterprise partners and to develop intelligence received from those partners for use by DHS and the IC. Also within DHS, the US Coast Guard Intelligence (CG-2) in the organization's unit was tasked with developing strategic, tactical, and operational intelligence related to the safety and security of the maritime domain, to support missions, and to inform decision-makers both within the Coast Guard and the Homeland Security Enterprise when developing policy with ramifications for maritime and port security.

The Central Intelligence Agency (CIA) is the agency that first comes to mind for most people when they think of the IC. The CIA is both a collection and an analytic agency and plays the leading and coordinating role in the collection of human intelligence or HUMINT.

Additionally, the CIA is the only intelligence agency authorized to carry out covert operations in foreign countries. The CIA is an independent agency, which, unlike the rest of the IC, is not subordinate to a cabinet official but rather accountable to the Director of National Intelligence, the National Security Council, and the president. This unique arrangement is a direct product of the National Security Act of 1947. The CIA is organized into five different directorates: the Directorate of Operations (DO), the Directorate of Analysis (DA), the Directorate of Science & Technology (DST), the Directorate of Support (DS), and the Directorate of Digital Innovation (DDI). The DO is arm of the CIA responsible for the coordination of covert operations and clandestine human intelligence collection across the IC. The DA uses information collected by the DO and other IC partners to analyze, produce, and disseminate all-source intelligence products on a wide variety of national security and foreign policy issues to consumers across the US government. Created in 2015, the DDI is the CIA's newest Directorate focusing on developing and implementing cutting-edge digital and cyber tradecraft and maintaining the agency's IT infrastructure (Central Intelligence Agency 2015).

Intelligence Sharing Within and Beyond the IC

There are also varieties of agencies at the federal level outside of the IC that have intelligence components. For example, in DHS alone, there is US Customs and Border Protection's (CBP) Office of Intelligence, Immigration and Customs

Enforcement (ICE) Office of Intelligence, and the Transportation Security Administration's (TSA) Office of Intelligence and Analysis (OIA) (to name a few). CBP's Office of Intelligence supports CBP's mission by providing intelligence in support or field operational capability, as well as strategic analysis focusing on terrorist, geopolitical, and economic threats to the agency's leadership, to aid in decision-making. ICE's Office of Intelligence (aka HSI-Intel) analyzes, produces, and disseminates strategic and tactical intelligence products to the agency's operational elements and leadership. The focus of these products includes identifying smuggling patterns, techniques and routes, and trends in criminal activity and predicting emerging and future threats. TSA's Office of Intelligence and Analysis (OIA) identifies security risks to prevent attacks against the US transportation system for a wide range of consumers (Cozine 2016).

Especially after September 11th, state and local law enforcement agencies began to take on a larger role as both producers and consumers of intelligence. Federal authorities became increasingly dependent on state and local agencies, and to a certain extent, private citizens to be their eyes and ears on the street and also their boots on the ground to carry out certain actions. Procedures had to be established in order to drive the intelligence collection, processing, and develop the intelligence communication systems of state and local agencies. Decision-makers at the state and local levels, and to a certain extent the private sector, also have become consumers of intelligence generated at the federal level. This dual role of state and local agencies as consumers and producers of intelligence presented a difficult problem – how can raw intelligence from all these diverse sources be collected, processed, analyzed, produced and disseminated in a timely manner? It quickly became apparent that the existence of effective intelligence fusion centers at the regional, state, and local levels of government was necessary for achieving this goal.

In this newfound role as both consumers and producers of intelligence, state and local agencies and various federal agencies outside the IC discovered a need to be able to share intelligence among both themselves and the IC itself. However, the sharing of intelligence among agencies, even within the IC, has a long history of being problematic. While the secrecy of intelligence, and the need to protect sources and methods of intelligence collection, certainly plays a role, another major issue that hampers intelligence sharing is that intelligence is often thought of as a commodity that has value and should be horded rather than shared. Intelligence agencies can often act as silos of intelligence and even within intelligence agencies separate silos may exist. This lack of intelligence sharing prevents those who may make the best use of available intelligence from receiving it. Even across and within law enforcement agencies, those in possession of valuable intelligence and information will hold onto it in hopes of getting a major arrest and all the notoriety that goes along with it.

Following the September 11th attacks, the 9/11 Commission (2004) concluded that the IC failed to connect the dots about al-Qaeda's plan to attack the United States by turning commercial airliners into weapons of mass destruction because pieces of information pointing to the plot were held by various agencies that, in hindsight, if connected, could have prevented it. This problem was compounded by the fact that there are a variety of agencies at the federal level that were not members of the IC but held important information. One example is the cases of two of the September 11 hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi. In early 2000, the CIA developed information that Mihdhar was a suspected al-Qaeda operative and he was previously issued a multiple-entry US visa. This intelligence was not shared with the US State Department, US Immigration and Naturalization Service (INS), and the US Customs Service (USCS). In late January 2000, Mihdhar and Hazmi both arrived in the United States and were allowed to enter the United States because the INS was not informed of Mihdar's terrorist connections. In late December 2000, the CIA and FBI developed information that connected Hazmi and Mihdhar with the man believed to be the mastermind of the US Cole attack in Yemen. Having left in June 2000, Mihdhar applied for and received a new visa in June 2001 and was allowed to enter the United States in July 2001 because both the State

Department and the INS were still unaware of his terrorist connections. It was not until August 23 that the CIA informed the State Department, FBI, INS, and USCS of the situation and recommended that Mihdhar and Hazmi be added to the watchlist databases as suspected terrorists. The FBI, upon learning of Mihdhar's entry on July 4, began searching for him in early September 2001 (Office of the Inspector General 2004). They did not share this information with any other federal, state, or local law enforcement agencies. These are just a few examples of how the lack of intelligence sharing hampered the ability of agencies to connect the dots of the attack on 9/11.

In its report, the 9/11 Commission stressed the need for all-source analysis across agencies because it is not possible to connect the dots without interagency cooperation. Likewise, there needed to be a better way to combined intelligence gathered overseas with information gathered domestically. The Commission also concluded that while the government has access to vast amounts of information and data, there lacked an effective system for processing and using it. The commission stated that the case of Mihdar and Hazmi demonstrated a system that requires a "need to know" before sharing. The Commission recommended information procedures be established to "provide incentives for sharing, to restore a better balance between security and shared knowledge and move from a culture of need-to know to a culture of need-to-share" (9–11 Commission 2004).

The concept of need-to-share was codified into law with the signing of the Intelligence Reform and Terrorism Prevention Act (IRATPA) of 2004, which also established the Information Sharing Environment (ISE) to facilitate the sharing of terrorist information. With the passage of the Implementing Recommendations of the 9/11 Commission Act in 2007, homeland security and weapons of mass destruction information were added to the ISE's portfolio. The mission of the ISE is to "[a]dvance responsible information sharing to further counterterrorism, homeland security, and counter weapons of mass destruction missions. Improve nationwide decision-making by transforming from information ownership to stewardship. Promote partnerships across federal, state, local, and tribal governments, the private sector, and internationally" (Office of the Director of National Intelligence 2019b).

One strategy that has been developed to link these potential sources together while simultaneously building the intelligence capacity of the fragmented US law enforcement community is the establishment of National Network of Fusion Centers. Intelligence fusion centers form a vital link between the federal intelligence community and state, local, and tribal levels of government. Fusion centers "are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding" (Department of Homeland Security 2018). Their areas of responsibility vary. Some are operated by states, others by large cities, and still others have a regional focus. Intelligence fusion centers also operate in different ways. Some fusion centers run 24/7, while others operate for only one or two shifts per day. The goal of fusion centers is to:

> [e]mpower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities. Provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. Conduct analysis and facilitate information sharing while assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism. (Department of Homeland Security 2018)

The need for intelligence sharing gets crowded even further when one considers the role of the private sector not just in the collection of intelligence but also as a potential consumer of intelligence. This need for intellignece sharing with the provate sector is greatest for those organizations involved in critical infrastructure protection as they are a highvalue target because if made incapacitated the effect would be devastating the overall health of the nation, particular if the effects of an attack cascaded to other areas within that sector or other sectors of critical infrastructure. At the heart of private sector intelligence sharing

regarding critical infrastructure are Information Sharing and Analysis Centers (ISACs). ISACs were established in 1998 to assist critical infrastructure owners and operators protect their facilities, personnel, and customers from a variety of threats and hazards by collecting, analyzing, and disseminating threat information to their members. ISACs are private organizations run by the owners and operators of critical infrastructure with the assistance and support of various federal, state, and local agencies. There are currently 21 sector-specific ISACs around the United States (National Council of ISACs 2019).

Conclusion

Intelligence allows its consumers, ranging from high-level policy-makers to frontline personnel, to make decisions, take action, consider possible alternatives, and predict possible outcomes.

The information needed to generate intelligence is collected through a variety of sources and methods within the five collection disciplines of HUMINT, OSINT, MASINT, GEOINT, and SIGINT. It is the intelligence cycle that is the process used to move from intelligence requirements set by the consumer to the finished intelligence that is produced and disseminated to the consumer to attempt to fulfill those requirements. The steps in this process include planning and direction; collection, processing, and exploitation; analysis and production; and dissemination. This methodical approach to creating intelligence to aid leaders and other decision-makers traces it root back to Sun Tzu and the *Art of War* and has been employed in the United States since the days of George Washington and the Revolutionary War. The approach to intelligence has evolved throughout US history as the threats faced by the nation change. It is likely that intelligence will continue to evolve as new threat emerge and the security environment changes.

Cross-References

- ▶ Border Security
- ▶ Critical Infrastructure protection
- ▶ Investigations: Terrorism
- ▶ Terrorism: Domestic
- ▶ Terrorism: Homegrown
- ▶ Terrorism: International

References

Althoff, M. (2015). Human intelligence. In M. M. Lowenthal & R. Clark (Eds.), *The five disciplines of intelligence collection* (pp. 65–80). Washington, DC: Sage.

Central Intelligence Agency. (2007a). *History of American intelligence*. Available at https://www.cia.gov/kids-page/6-12th-grade/operation-history/history-of-american-intelligence.html

Central Intelligence Agency. (2007b). *History of the CIA*. Available at https://www.cia.gov/kids-page/6-12th-grade/operation-history/history-of-the-cia.html

Central Intelligence Agency. (2015). *Today's CIA*. Available at: https://www.cia.gov/about-cia/todays-cia

Cozine, K. (2015). Setauket to Abbottabad: The value of film and television in teaching human intelligence. *Journal of Strategic Security, 8*(3), 80–92.

Cozine, K. (2016). Fragmentation and interdependency: Border security intelligence in North America and Europe. *The International Journal of Intelligence, Security, and Public Affairs, 18*(3), 175–197.

Cozine, K. (2017). Teaching the intelligence collection disciplines: The effectiveness of experiential learning as a pedagogical technique. *Global Security and Intelligence Studies, 2*(2), 4.

Defense Intelligence Agency. (n.d.). *About DIA*. Available at https://www.dia.mil/About/

Department of Homeland Security. (2018). *National network of fusion centers fact sheet*. Available at: https://www.dhs.gov/national-network-fusion-centers-fact-sheet

Federation of American Scientists (FAS). (1995). Introduction to the intelligence cycle. Available at: https://fas.org/irp/doddir/army/miobc/intcyclp.htm

Lahneman, W. (2017). The seven-step intelligence cycle. *The Center for Homeland Defense and Security.* Available at: https://www.chds.us/coursefiles/NS4156/lectures/intel_7_step_intel_cycle/script.pdf

Lowenthal, M. M. (2020). *Intelligence: From secrets to policy* (8th ed.). Thousand Oaks: CQ press.

Morris, J., & Clark, R. (2015). Measurement and signatures intelligence. In M. M. Lowenthal & R. M. Clark (Eds.), *The five disciplines of intelligence collection* (pp. 159–208). Washington, DC: Sage.

Murdock, D., & Clark, R. (2015). Geospatial intelligence. In M. M. Lowenthal & R. M. Clark (Eds.), *The five disciplines of intelligence collection* (pp. 111–158). Washington, DC: Sage.

National Commission on Terrorist Attacks Upon the United States. (2004). Final report of the National Commission on Terrorist Attacks Upon the United

States. Available at: https://govinfo.library.unt.edu/911/report/911Report.pdf
National Council of ISACs. (2019). *ABOUT ISACs*. Available at: https://www.nationalisacs.org/about-isacs
National System for Geospatial Intelligence. (2018). Geospatial Intelligence (GEOINT) Basic Doctrine. Available at: https://fas.org/irp/agency/nga/doctrine-2018.pdf
Nolte, W. (2015). Signals intelligence. In M. M. Lowenthal & R. M. Clark (Eds.), *The five disciplines of intelligence collection* (pp. 81–110). Washington, DC: Sage.
Office of Naval Intelligence. (n.d.). *Intelligence community agencies*. Available at: https://www.oni.navy.mil/Intelligence-Community/IC-Agencies/
Office of the Director of National Intelligence (ODNI). (2019a). *About the ISE*. Available at: https://www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise/ise-mission-vision
Office of the Director of National Intelligence (ODNI). (2019b). The National Intelligence Strategy of the United States of America. Available at: https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf
Office of the Director of National Intelligence (ODNI). (2019c). *What is intelligence*?. Available at: https://www.dni.gov/index.php/what-we-do/what-is-intelligence?highlight=WyJzaWdpbnQiXQ==
Office of the Inspector General. (2004). A review of the FBI's handling of Intelligence information related to the September 11 attacks. Available at: https://oig.justice.gov/special/s0606/chapter5.htm
S. 2845 (108th) Intelligence Reform and Terrorism Prevention Act of 2004. Available at: https://www.congress.gov/bill/108th-congress/senate-bill/2845

Further Reading

Logan, K. G. (Ed.). (2017). *Homeland security and intelligence*. ABC-CLIO. Santa Barbara.
Steiner, J. E. (2014). *Homeland security intelligence*. Thousand Oaks: CQ Press.

Internet (Deep and Dark Web)

Douglas E. Salane
Mathematics and Computer Science Department,
John Jay College of Criminal Justice,
New York, NY, USA

Keywords
Internet of things · Search engines · the Web · Social networks · World-Wide-Web

Definition

The Internet is a global computer network that interconnects over 23 billion digital devices (Statista 2018).

Introduction

Originally intended to interconnect just a few hundred mainframe computers in universities and corporate and government labs, the Internet now enables desktops, laptops, cell phones, and just about anything that contains a processor to access information or connect with other devices anywhere in the world. Often categorized as the Internet of Things (IoT), in recent years billions of devices such as consumer appliances, sensors, and even medical devices have been connecting to the Internet. These devices soon will outnumber computers (Tung 2017a). Estimates show that by 2020 there will be four devices connected to the Internet for every person on Earth (Tung 2017b).

The Internet is, however, much more than a physical global network for interconnecting devices. The Internet also provides the essential services that allow software applications and devices to function together and exchange information reliably. Internet communication protocols have allowed developers to produce the Internet applications upon which we now rely: the web, search engines, social networks, and many other web applications. Services include an addressing and naming system so devices can locate each other, mechanisms for reliable transmission of information over what is essentially an unreliable, best effort delivery network, and even mechanisms for ensuring that information stored in different formats on different devices can be interchanged. Without such services, applications such as the World Wide Web would not exist.

Internet History and Development

Much of the underlying Internet technology was developed over 30 years ago in several US government-funded projects (Leiner 1997). In the 1960s and 1970s, the Defense Advanced Research

Projects Agency funded the initial prototype network known as the ARPANET, an effort to connect multiple heterogeneous networks through a system of gateway computers. In 1983, the ARPANET made the transmission control protocol/Internet protocol (TCP/IP) the standard communication protocols used in the network. Thus hosts and networks that made used TCP/IP standards could be added to the ARPANET.

In the mid-1980s, the National Science Foundation played a key role with its funding of NSFNET whose purpose was to interconnect supercomputing facilities at government laboratories and universities (National Science Foundation 2018). This project led to the development of a backbone network for the Internet and demonstrated its utility. The program paved the way for the transition to current model where private telecommunication companies provide most of the Internet network infrastructure and the service fees they charge finance infrastructure maintenance and development.

Today the Internet is a complex system of interconnected networks mostly owned by private sector telecommunication companies known as Internet Service Providers (ISPs). In some countries the networks are government owned and controlled. There are local and regional service providers as well as core service providers who interconnect regional providers and offer a type of backbone for the Internet. Moreover, in recent years, major content providers such as Google have developed their own global networks separate from the public Internet to interconnect their data centers. These content provider networks connect to ISPs to access the public Internet and attempt to avoid using the Internet core where possible. Typically, they rely on the public Internet to reach end users (Google 2018).

Internet Technology

The Internet designers introduced a number of network technologies and made a number of technical decisions that have allowed the Internet to scale from a few hundred machines to billions of devices (Leiner 1997). One key technology was the packet-switched network. In such networks, a large file to be transmitted, for example, is broken into multiple packets which are then transmitted over the network and reassembled at the destination. Packets may not even follow the same path from source to destination. A second crucial idea was to keep the complexity and computation at the end points. Most processing involved in moving traffic is done at the sending and receiving end points, with minimal processing on gateway devices that move traffic through the network. This was a departure from the way telecommunications worked at the time where if a sender and receiver wanted to communicate, intermediate switches had to be configured to make the connection. A third key component was the Internet addressing and routing systems that allowed networks to be added to the Internet with minimal impact on the existing system.

Of course, the Internet has benefited from the incredible increase in computational powered realized during the past 30 years. The switches and routers, key building blocks that move traffic, have increased in speed by at least three orders of magnitude during this period. Nonetheless the decision to keep processing on intermediate switching/routing devices to a minimum is a key factor in the scalability of the network. In addition, separating the physical network layer from other network layers allowed the massive investment in software applications at the network, and transport and application layers of the network to remain in place as underlying network hardware technologies evolved and improved.

From the beginning the technical specifications have largely been in the hands of committees of stakeholders who work together to devise the open or publicly available communication protocols and specifications needed to make the Internet work. With open protocols talented programmers anywhere in the world could develop network services and applications and improve on existing software.

Internet Management and Governance

Governance of a valuable shared resource such as the Internet, a critical information infrastructure for commercial activity and many competing

interests, requires technical standards as well as policies needed to address issues such as privacy, security, and access (Global Commission on Internet Governance n.d.). As a global system, the Internet has no central manager or authority. Each nation oversees the activities that take place on the Internet in that country – some are very open, while others are highly regulated. In addition, the private sector plays a key role through user terms of service agreements both for Internet access and use of various web applications. From the beginning, technical standards have followed the multi-stakeholder approach, a distributed form of governance that includes developers, users, and others with an interest.

The Internet Society (Internet Society 2018) is the umbrella organization that provides a home for and financial support for the Internet standards process. Two organizations manage the actual development of technical standards, the Internet Engineering Task Force (IETF), which oversees the development of detailed technical protocol standards, and the Internet Architecture Board (IAB), which considers the longer-term development of the Internet. The IETF publishes a set of technical protocol standards called Requests for Comments (RFPs) which define the standards for communication protocols and many Internet applications (IETF 2018). Another key organization, the Internet Corporation for Assigned Names and Numbers (ICANN), manages the Internet/Domain Name System, which provides names and addresses for Internet computers and services (ICANN 2018).

Two contentious Internet governance issues concern access and privacy. The net neutrality debate centers on the ability of an ISP to prioritize Internet traffic and provide higher levels of service for customers willing to pay for it. The fear is that customers who cannot afford a premium service will receive a lower level of service and be denied the full utility of the Internet. The European Union supports net neutrality (European Commission 2018a), while the Federal Communications Commission in the USA recently started allowing ISPs to charge more for preferred services. The issue of ISPs making use of customer data is being addressed by a number of states in the USA with some states passing legislation to restrict ISPs from accessing customer data without their explicit permission (National Conference of State Legislatures 2018). The European Union has a strict privacy regime which regulates the way ISPs and Internet search and social network companies handle user data (European Commission May 23, 2018b).

Deep and Dark Web

The deep web and the dark web characterize portions of the World Wide Web. Many conflate the two terms, but there is a distinct difference. Many consider the dark web to be a subset of the deep web. Both terms refer to web sites not generally accessible to search engines. Access to dark web sites requires special software which protects the anonymity of the both the web site and the browser computer. Web sites readily accessible to search engines and indexed by them are often referred to as being part of the Surface Web, which most estimates put at under 5% of the entire World Wide Web.

The deep web includes web pages that cannot readily be accessed by search engine web crawlers. Thus such pages are not indexed and won't appear in a list of search results. Examples of such pages include those protected by captchas, pages that require a user login, pages returned when one fills out a form, or paywall-protected digital media content.

Access to dark web sites typically requires the use of the Tor browser (TOR 2018). This browser makes it very difficult for someone monitoring a network to identify the address of either the browser or the web site being accessed. TOR often is used to browse the Surface and deep web as well when anonymity is desired. Dark web users often take the extra precaution of using a virtual private network for additional assurance of anonymity.

Dark web sites don't use extensions such as .org or .com but .onion, which is not part of the Internet/Domain Name System. Sites available on the Surface Web provide lists of sites in the dark web. The anonymity afforded by the dark web makes it widely used for nefarious activities including black markets, botnet operations, selling hacking services and malware, and a range of

criminal activities. In addition, dark net sites also host whistleblowing forums and political discussion groups that might be suppressed in certain countries.

Conclusion

The Internet and the applications it supports are critical to economic and social activities throughout the world. As an indication of how much the world has grown to rely on the Internet as an information source, Google currently processes over 3.5 billion searches each day up from about 3.5 million per day when it was founded in 1998 (Internet Live Stats 2018). In less than a generation, Internet-based applications such as social networks, search engines, online shopping and advertising, e-mail, and other applications have created entirely new industries and changed the way organizations and people interact and get information. A key challenge now is the governance of this shared resource so it continues to spawn innovation and development and at the same time protects the security of its users and makes the Internet work for everyone (Internet Society 2017).

Cross-References

- ▶ Criminals: Cybercriminals
- ▶ Cybersecurity: Policy
- ▶ Cybersecurity: Practice
- ▶ Internet of Things

References

European Commission. (2018a). *Open Internet*. Retrieved from https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality

European Commission. (2018b, May 23). *Data Protection in the EU*. Retrieved from European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Global Commission on Internet Governance. (n.d.). *Who runs the Internet? The global multi-stakeholder model of Internet governance*. Ottawa: Centre for International Governance Innovation and the Royal Institute of International Affairs.

Google. (2018). *Our Infrastructure*. Retrieved from Google: https://peerig.google.com/#/infrastructure

ICANN. (2018). *Get Started*. Retrieved from ICANN: https://www.ican.org/get-started

IETF. (2018). *Internet Standards*. Retrieved from https://www.ietf.org/standards/

Internet Live Stats. (2018). *Google Search Statistics*. Retrieved from Internet Live Stats: http://www.internetlivestats.com/google-search-statistics/

Internet Society. (2017). *2017 Global Internet Report: Paths to Our Digital Future*. Retrieved from Internetsocity.org: https://www.internetsociety.org/globalinternetreport/?gclid=EAIaIQobChMIzJbOwqiL3QIVix-GCh0c5AGHEAAYASAAEgI9X_D_BwE

Internet Society. (2018). *About the Internet Society*. Retrieved from Internet Society: https://www.internetsociety.org/about-internet-society

Leiner, B. C. (1997). *Brief History of the Internet*. Internet Society. Retrieved from https://www.internetsociety.org/internet/history-internet/brief-history-internet/

National Conference of State Legislatures. (2018). *Privacy Regulation Related to Internet Service Providers*. Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx

National Science Foundation. (2018). *A Brief History of NSF and the Internet*. Retrieved from National Science Foundation: https://www.nsf.gov/news/special_reports/cyber/internet.jsp

Statista. (2018). *Internet of Things connected devices installed base world wide from 2015 to 2025*. Retrieved from Statista: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

TOR. (2018). *What is the Tor Browser*. Retrieved from TOR: https://www.torproject.org/projects/torbrowser.html.en

Tung, L. (2017a, Feb 7). *IoT Devices will outnumber the world's population for the first time this year*. Retrieved from ZDNet: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

Tung, L. (2017b, Feb 7). *ZDNet*. Retrieved from IoT Devices Wil Outnumber the World's Population for the First Time This Year: https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

Further Reading

Finklea, K. (2017, Mar 10). *Dark Web*. Congressional Research Service. Retrieved from Congressional Research Service: https://fas.org/sgp/crs/misc/R44101.pdf

Internet of Things

Marie-Helen Maras
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Internet of Things · Privacy · Security

Definition

The Internet of Things (IoT) is an umbrella term used to describe a network of Internet-connected devices that collect, store, collate, analyze, and share a significant amount of information and monitor people, animals, plants, and/or objects in order to provide users of these devices with some form of service.

Introduction

The Internet of Things (IoT) is an umbrella term used to describe a network of Internet-connected devices that are designed to provide users of these devices with some form of service. In order to provide this service, these devices collect vast quantities of data about users and contextual data from these devices, and process, aggregate, and analyze this data. The data collected and processed is known as *big data*, "extremely large data sets that can be analyzed to reveal patterns, trends and associations, especially relating to human behavior and interactions" (Maras and Wandt 2019, p. 162). The contextual information from these devices is obtained through the real-time, continuous, and remote monitoring of everyday objects, plants, animals, and/or people (Maras 2015). The contextual information obtained from IoT devices enables them to make decisions independent of the users. An example of such a device is Amazon's Dash Smart Shelf, which identifies drops in the weight of supplies on the shelves and automatically reorders the supplies that need replenishing from Amazon (Haselton 2019). Ultimately, the Internet of Things, as envisioned, will consist of Internet-connected devices that, like Amazon Dash, will be able to make decisions primarily independent of any user input and predominately without the need for user input.

Security and Privacy Concerns

IoT devices were built with efficiency in mind and not security (Maras 2015). There are security risks associated with the use of this technology. The devices are vulnerable to unauthorized access and modification of features and services provided through hacking, and often include hard-coded passwords and backdoors that can be exploited by cybercriminals (Maras 2015). In the United States, there is currently no federal regulation of IoT devices. States, like California and Oregon, however, have passed legislation requiring manufacturers to include security features in IoT devices. For instance, California's 2019 law (Senate Bill No. 327) requires manufacturers "to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure." In the European Union, a law was passed, the EU Cybersecurity Act of 2019, that, among other things, called for establishing a cybersecurity certification framework in the EU for digital technologies (see EU Regulation 2019/881). This law is designed to enhance consumer trust in devices and security of technological devices.

IoT devices were also not built with privacy in mind (Maras 2015). A person's privacy can be violated because the data collected, stored, collated, and shared by IoT devices can reveal personal information (or data) about the users of these devices. Depending on the device, this

can include (but is not limited to) a person's movements, habits, routines, hobbies, personal preferences, physical activities, eating habits, sleeping patterns, and even medical information. Users of IoT devices often have little, if any, control and choice over the data that is obtained, aggregated, analyzed, and shared about them and knowledge of the quantity and types of data that is shared about them. To date, IoT devices are not predominately created with privacy-enhancing features built into the architecture of these devices to minimize the collection of data by these devices from the outset (a form of *privacy by architecture*). Instead, what is observed is *privacy by policy*, whereby privacy-enhancing applications are considered post-design to manage the data already collected, stored, and potentially shared by these devices (e.g., notices of data management practices and data management user interfaces). In the European Union, the General Data Protection Regulation (GDPR) of 2018 (EU Regulation 2016/679) also does not impose any obligations on IoT manufacturers to implement technological data protection measures. While the United States similarly does not have a federal law mandating data protection measures by IoT manufacturers, state law does exist. A case in point is the California Consumer Privacy Act (CCPA) of 2018 (Senate Bill No. 1121), which provides California residents with rights over the collection and use of their personal data (Schwartz et al. 2018). As of 2020, laws, such as the CCPA, are the exception in the United States, not the norm.

Conclusion

Everyday objects are increasingly being connected to the Internet in order to collect, store, collate, analyze, and share substantial quantities of data about IoT devices, users of the devices, and the environments within which these devices operate, as well as to facilitate the monitoring of people, animals, plants, and/or objects (which one or ones are monitored depends on the IoT device). IoT devices raise security and privacy concerns that have not yet been adequately addressed.

Cross-References

▶ Big Data

References

Haselton, T. (2019, November 21). Amazon announces a 'smart' shelf that automatically buys new office supplies when you run low. *CNBC*. https://www.cnbc.com/2019/11/21/amazon-dash-smart-shelf-reorders-office-supplies-for-you-automatically.html

Maras, M.-H. (2015). The Internet of Things: Security and privacy implications. *International Data Privacy Law, 5*(2), 99–104.

Maras, M.-H., & Wandt, A. S. (2019). Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy, 4*(2), 160–177.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Schwartz, A., Tien, L., & McSherry, C. (2018). How to improve the California Consumer Privacy Act of 2018. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018

Further Reading

Maras, M.-H. (2015). The Internet of Things: Security and privacy implications. *International Data Privacy Law, 5*(2), 99–104.

Maras, M.-H., & Wandt, A. S. (2019). Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy, 4*(2), 160–177.

Interviewing Adults: Communication at the Front Line

R. Milne[1], A. Shawyer[1], G. Dalton[1], B. May[1], J. Nunan[1] and R. Bull[2]
[1]Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, UK
[2]University of Derby, Derby, UK

Keywords
Emergency · Information · Decision-making · Questioning · Rapport

Definition

Interviewing adults refers to the use of research-based methods for obtaining reliable information needed for critical decision-making during the course of an emergency.

Introduction

The key to ensuring successful outcomes within the emergency services, be it a fire, trauma, or criminal in nature, is in part reliant on gaining reliable information (Nunan et al. 2016). Reliable information may in turn aid effective, critical decision-making throughout an emergency (Alison et al. 2015). However, obtaining such information is a complex task, especially at the front line where the event is often surrounded by chaos and confusion and where there are limited fast-time resources (Dalton et al. 2018). Thus, the information-gathering task is confounded by numerous factors, but in the current entry, we will focus on three key areas of research: (i) the source of the information (i.e., is it a witness, victim, or emergency services personnel themselves?); (ii) the types of questions used to gather the information (i.e., open questions or leading questions); and (iii) the manner in which the questions are asked (i.e., has rapport been developed?). The enormity of this task in these dynamic circumstances should not be underestimated. It is essential that researchers explore the nature in which this information is gathered to help devise workable recommendations and techniques that aid the blue light services to work efficiently and effectively. By utilizing the knowledge underpinning the psychology of communication and the fallibility of memory, well-researched concepts in the psychological literature can help us advise on the best means of gathering full and reliable information and develop tools to assist in this process. Fortunately, with the ever-increasing demand for research development in the domain of blue light services, academic-practitioner collaboration is becoming more commonplace. There is a history of sharing knowledge in respect to information-gathering and decision-making with practitioners across a range of domains (e.g., Alison et al. 2015; Cohen-Hatton et al. 2015). However, we must not be complacent; there is still scope for learning and development.

This entry is structured around the different emergency services themselves, starting with (i) the police, examining frontline communication, and dealing with critical incidents. The entry then examines the limited amount of work concerning (ii) paramedics. Communication and information-gathering are used within this type of organization for different reasons to the police (i.e., potential medical intervention). Finally, (iii) the Fire and Rescue Service, whereby good communication in this domain provides crews with the necessary information to ensure operational competence and effective risk assessment and maximize crew, witness, and victim safety, is described.

Police: Frontline Communication and Critical Incidents

Following an initial call to the emergency services (see Dalton and Milne in press, for more in this area), frontline police officers will often attend a scene to establish (i) initial response requirements, (ii) what has happened, and (iii) who is likely responsible (Milne and Bull 2006, 2016). Thus, it is important that police officers are able to interview witnesses and victims about what they can remember. However, this poses challenges because extracting reliable information from memory at the scene of an incident can lead to both encoding errors (e.g., witnesses reporting details they did not experience) and retrieval errors (e.g., police officers asking inappropriate questions that lead to inaccurate information; Snook et al. 2012). The latter is a great risk for frontline police officers who typically have the least amount of training and experience (Dando et al. 2009). These challenges are extenuated given that frontline officers are often in resolution mode, dealing with dynamic events (e.g., separating a couple involved in a domestic) as opposed to an investigative mode (e.g., gathering information from those involved). The situation requires officers to be in both resolution and investigative mode, a cognitively demanding task (Dalton et al. 2018). There is limited field research looking

at police interviewing at the scene of the investigation. The few field studies that have been conducted have found shortcomings in the way in which police officers interview witnesses, including the overreliance on asking closed questions (Myklebust and Alison 2000) and using leading questions (Wright and Alison 2004). Police officers themselves have reported feeling inadequately trained, ill-equipped, and under pressure when conducting such interviews (Dando et al. 2009).

Due to government cuts and the need for police forces to modernize, the use of technology by the police has increased significantly (Jennings et al. 2014). From police dashcams to the issuing of personal body-worn video cameras, the police are now more accountable for their actions. Body-worn video cameras are attached to the uniform of frontline officers, and, when turned on, these provide a reliable record of all interactions that take place at the scene (e.g., with witnesses, victims, suspects, and/or emergency services personnel themselves). As a result, the recording of such interactions offers a unique insight for researchers into what occurs at the scene of an incident. More specifically, and for the first time, academics and practitioners are now able to obtain an accurate representation of the communication used including the questions frontline police officers ask when in attendance at an incident. To date, research suggests that frontline officers often fail to deploy strategies to build rapid rapport with witnesses and tend to use inappropriate questions (e.g., leading) to gather information (Dalton et al. 2018; Gabbert et al. 2016).

To examine frontline communication, Dalton et al. (2018) were granted privileged access to body-worn video footage over 15 months. This piece of research examined how frontline police officers interviewed witnesses and victims at the scene of an incident. The main objective was to explore how frontline police officers elicited person descriptions about the suspect(s). The research further investigated the impact of contributing factors (e.g., witness intoxication, stress, and vulnerability) on attaining these descriptions. Finally, the practicalities of using body-worn video were documented, such as the quality of the audio and lighting and camera angle. It was found that person descriptions were being elicited using inappropriate questions and that this had the potential to produce vague or incorrect descriptions. However, when appropriate questions were used, witnesses provided a significantly higher number of descriptors. Thus, asking the right questions is key. Decisions are only as good as the information that is fed into making them. That information is only as good as the questions asked. Poor questioning can lead to poor information that can lead to poor decision-making.

The collaboration between academics and practitioners in this area of the emergency services has been fruitful, and a number of tools have been developed. This includes research-based tools and techniques for eliciting information from cooperative adult interviewees. In incidents where there are mass witnesses (e.g., a terror attack; see next subsection), two of the main issues are a lack of time and resources. The Self-Administered Interview (SAI; Gabbert et al. 2009) is a paper-based interview that can be given out at the scene of the incident and is a protocol of instruction and questions that is designed to elicit a written free-recall statement. Studies using the SAI have reported a significant increase in the completeness and accuracy of information (Gabbert et al. 2009; Krix et al. 2016). Moreover, the SAI protects the memory from potentially distorting post-event information (Gabbert et al. 2009, 2012; Hope et al. 2014).

If face-to-face interviews are required, then frontline officers need to be asking the right questions. Working with practitioners, Gabbert et al. (2016) developed an evidence-based Structured Interview Protocol (SIP) and related training, for use by frontline police officers. SIP is based on the premise that the best information is that gathered by open-ended questions (e.g., Tell me what happened), followed by specific-closed questions (e.g., When was that?). The SIP package promotes high-quality interview performance, reduces memory contamination, and has led to increased use of rapid rapport techniques, enhanced "engage and explain" skills, and an increase in appropriate question types, used in a structured manner. Another technique that enhances memory

retrieval during frontline communication is the use of a sketch plan. Sketch plans have been shown to be useful in helping witnesses to explain what they experienced and the location of people and objects (Dando et al. 2009). Research has also shown that sketches can be used with a variety of witnesses, including those who are deemed vulnerable (Mattison et al. 2018).

Terrorism has also added challenges to how police communicate at the front line, especially where mass witnesses are involved. Experiencing trauma is a major concern in all critical incidents (Smith and Milne 2018). In such situations, casualty/witness interviewing is complex because of the confusion and chaos surrounding the event, limited fast-time resources, and the scale of the problem. In addition, gaining reliable information from witnesses to inform the emergency services while taking heed of their trauma is a difficult task and can be compromised by poor interviewing or greatly enhanced with good sensitive interviewing (Smith and Milne 2018). Getting the investigation into terrorism wrong, however, has far-reaching costs to society, not only psychologically but also economically. For example, in one report it has been estimated that one million fewer people visited Paris following the terror attacks, a cost of £644 million (Harris 2016). Getting it right is crucial in ensuring a safe and resilient society.

To ensure best practice, academics and police have worked together examining the challenges involved in managing such critical incidents. For example, Smith and Milne (2018) developed a framework for triaging mass witnesses based on their own experience of dealing with such an incident and a dialogue with police interview advisers involved in developing strategies for this type of investigation. Witness Interview Strategies for Critical Incidents (WISCI) sets out to describe the various considerations needed to develop a witness interview strategy for a critical incident involving multiple witnesses, a triage system. The number of witnesses to some high-profile critical incidents is such that it is usually necessary to put an organizational structure in place to facilitate their management (Smith and Milne 2018). It is only by the development of such an organizational structure that the investigation team can have any hope of managing a large volume of witnesses. Witness interview strategies for high-profile critical incidents use the same framework that is used by witness interview strategies more generally (see Smith and Milne 2018). This framework consists of the following: (i) initial contact, (ii) investigative interviews, and (iii) post-interview process and product. Of particular importance is the fact that critical incidents are characterized by trauma. Thus, understanding how to manage trauma is essential for interviewers. Interviewers must be "open, flexible, and able to adapt to the state and expressions of the interviewee" to achieve rapport and allow them to feel in control of the information flow (Risan et al. 2016, p. 414). Such a skill hinges on the ability to manage emotions. The ability to manage emotions is central to the concept of emotional intelligence which involves "the ability to recognise, appraise and understand emotions on the basis of verbal and non-verbal expressions, to use emotions to enhance one's thinking through reasoning or problem-solving, and to manage emotional responses" (Risan et al. 2016, p. 415). WISCI is a good example of how practitioners and academics can work together to develop a realizable working framework in response to a real-world problem. Another emergency service organization always in attendance at critical incidents is paramedics. It is to this group that we now turn.

Paramedics: Multiagency Working

There is limited work looking at the frontline communication of paramedics. As can be seen from the prior discussion, in the course of a major incident, the collection and dissemination of relevant and reliable information are crucial to an effective and efficient multiagency response (Allen et al. 2014). The techniques used to elicit and share information are, therefore, key to the success of working in harmony (Waring et al. 2017). However, similar to the police (outlined above), a number of factors may impact upon this process within this service, such as (i) the sources of the information and (ii) the communication methods used to gather the information (e.g., open, closed, or leading questions).

Simulation exercises are a method used to help emergency services hone their skills. Training in a realistic simulated environment provides a safe place to gain experience and develop skillsets ready for real incidents (Alison and Crego 2012; Rouse 1991). Exercise Unified Response (EUR), Europe's largest major incident training exercise to date, provided a rich environment for the emergency services to test their multiagency response (London Fire Brigade 2017). The simulation, which lasted 4 days, consisted of a collapsed building that mirrored London Waterloo Underground Station. This project involved all the emergency services as well as members of the public who acted as casualties. This exercise demanded a timely and effective short-term response from the emergency services together with an efficient long-term plan of action.

Body-worn video cameras were used in partnership with London Ambulance Service (LAS), to examine frontline communication (both within and across LAS teams) and the emergency response (Nunan et al. in press). The research focused on day 1 of EUR to capture the initial frontline communication and decision-making in response to the major incident. The project aimed to (i) produce timelines of key stages of LAS's emergency response to highlight successes and challenges faced during the golden hour and the actions of specialist teams, such the Hazardous Area Response Team (HART) throughout day 1 (see Nunan et al. (2016) described later – for similar methodology with the fire service), and (ii) examine LAS's use of multiagency communication and information sharing. LAS's main priority is the preservation of life. Furthermore, the psychological and physical well-being of the casualty may inhibit the collection of crucial information due to the possible onset of trauma and the unconscious state of some casualties.

Nonetheless, the information collected is only as reliable as the techniques used to elicit that said information. Importantly it was found that the importance of successful multiagency working could not be overstated. Underpinning successful multiagency working is the use of effective communication (Waring et al. 2017), which is implemented through information sharing (Allen et al. 2014), joint risk assessments, and timely command meetings. It was also recommended that multiagency talk groups should be utilized more frequently and used to complete a joint risk assessment. In addition, it was outlined that training in areas such as communication skills and detailed briefings should enhance the frontline response.

Nunan et al. (in press) also demonstrated that body-worn cameras can be used as an effective service evaluation tool to examine real-world practices. Body-worn cameras are able to timestamp and capture both live time communication and behaviors during training exercises, which could be revisited and shown as training material or subjected to research analysis (Nunan et al. in press). Body-worn cameras can promote best practice, identify training needs, and highlight areas for future evaluation. The next emergency service to be examined is the Fire and Rescue Service. Are appropriate communication strategies pivotal to this line of business too?

Fire and Rescue Service: Control Room Communication

Information is also the lifeblood of the Fire and Rescue Services, as it provides operational (and nonoperational) crews with the necessary information to ensure operational competence and effective risk assessment, maximizing crew, witness, and victim safety (e.g., Cohen-Hatton et al. 2015). For example, information pertaining to the location of an incident, establishing the type of incident, and identifying potential casualties and risks are elicited in the control and command center during an emergency response call. However, despite regular developments in control and command (e.g., Fennell 1988; London Fire Brigade 2017; National Operational Guidance Programme 2019), attaining incident-relevant information remains a difficult task.

Operational crews in the control and command center (i.e., control room officers) collect a vast quantity of information, and as with similar blue light services, the use of appropriate question types (e.g., open, specific-closed, etc.) impacts upon the quality of the information gained

(Leeney and Mueller-Johnson 2012). Additionally, it is the responsibility of the control room officer to carefully choreograph the movements of each operational appliance and subsequent crew while simultaneously imparting safety advice to those in jeopardy and gathering critical information from witnesses and victims (National Operational Guidance Programme 2019). The multifaceted role of the control room officer, therefore, is often challenging, diverse, and complex and requires an aptitude to effectively and efficiently make decisions based on the information they have gathered. However, gathering reliable information and undertaking effective decision-making that preserves life, prevents injury, and minimizes property damage are cognitively, emotionally, and physically difficult (e.g., van den Heuvel et al. 2013).

Our natural ability to communicate is not conducive to the scenarios faced by control room officers (or any frontline communicator). Control room officers are often faced with high-stake situations, requiring responsive action in short time frames and dealing with people who are often in heightened emotive situations – all factors which do not often occur in everyday communication interactions (Cohen-Hatton et al. 2015). Furthermore, everyday communication incorporates question types (e.g., leading), which are inappropriate for Fire and Rescue Services, indeed, for any emergency services in an operational role. This is because everyday communication is not aimed at gathering reliable information at speed. To the contrary, everyday language includes questions which are often time-consuming and do not translate to information-gathering tasks during high-stake situations (e.g., Leeney and Mueller-Johnson 2012). Therefore, using the right question types to gather accurate information is a skill that must be learned and nurtured if the Fire and Rescue Service (or indeed any service) is to further develop their control and operational crew communication.

Research conducted via body-worn cameras attached to London Fire Brigade frontline responders during EUR (as explained above) examined frontline communication and the handover of information over time (Nunan et al. 2016). This project offered an insight into the communication strategies employed in fire and rescue personnel frontline communication and demonstrated what happens when a part of the communication chain is broken. A breakdown in frontline communication adversely affects the reliability of the information collected, the sharing of such information, and the quality of subsequent decisions. It is evident, therefore, that training is required in areas such as communication skills, effective questioning of civilians, and detailed briefings (Nunan et al. 2016). Furthermore, this project demonstrated the effectiveness of evidence-based tools (e.g., body-worn video), to observe frontline communication, with the purpose of supporting, developing, and enhancing frontline communication and response (Nunan et al. 2016).

In response to those initial findings (Nunan et al. 2016), and in collaboration with Fire and Rescue Services across the United Kingdom, research has assessed communication in the control and command center (Shawyer et al. in preparation). With privileged access to control and command emergency recordings, alongside a survey to establish perceptions and understanding of questioning techniques, rapport building techniques, and barriers to communication, the present research focused on working toward the development of a bespoke communication protocol. Initial findings from the first phase of this research have suggested that a number of barriers to optimum communication exist: a combination of individual and situational factors. For example, a stressed and confused caller, with a patchy mobile phone signal, trying to adapt to the control officer's agenda (e.g., the location of the incident, alongside the nature of the incident) and questioning, can all hamper attempts to gather reliable and incident-relevant information in a timely manner. An examination of the emergency recordings also revealed communication in the control and command center may not always have been wholly effective; that is, the communication strategies used to elicit information sometimes relied on the use of ineffective question types (e.g., leading, closed, forced choice questions), similar to that found in previous research (e.g., Leeney and Mueller-Johnson 2012). This project has demonstrated a need for additional

support, development, and enhancement in communication techniques in control and command center staff. It also provides initial insight into the potential barriers which can impact of the effectiveness of control and command communication and decision-making.

Conclusion

This entry has explored how the emergency services communicate at the front line. While each service is responsible for gathering different types of information pertinent to them, it is clear that all face similar challenges. For example, research across the emergency services has highlighted the need to ask the right questions, in the right manner. Thus, asking open-ended questions and developing rapport are key to gathering reliable information. The entry has also identified a number of tools that have been designed in partnership between academics and practitioners to aid and improve information-gathering by the emergency services. Finally, the use of technology and specifically body-worn cameras can be "an effective research tool to examine front-line communication, promote best practice, highlight areas for future training needs, and further research areas" (Nunan et al. 2016, p. 52).

Cross-References

- First Responders: Police
- Interviewing Children
- Investigations: Accidents and Reconstructions
- Investigations: Criminal
- Investigations: Terrorism
- Private Detectives
- Public-Private Partnerships: Training and Coordination in Disasters

References

Alison, L., & Crego, J. (2012). *Policing critical incidents: Leadership and critical incident management*. London: Routledge.

Alison, L., Power, N., Heuvel, C., Humann, M., Palasinksi, M., & Crego, J. (2015). Decision inertia: Deciding between least worst outcomes in emergency responses to disasters. *Journal of Occupational and Organizational Psychology, 88*(2), 295–321. https://doi.org/10.1111/joop.12108.

Allen, D. K., Karanasios, S., & Norman, A. (2014). Information sharing and interoperability: The case of major incident management. *European Journal of Information Systems, 23*(4), 418–432. https://doi.org/10.1057/ejis.2013.8.

Cohen-Hatton, S. R., Butler, P. C., & Honey, R. C. (2015). An investigation of operational decision making in situ. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 57*(5), 793–804. https://doi.org/10.1177/0018720815578266.

Dalton, G., & Milne, R. (in press). Interviewing witnesses and victims of crime. In P. Marques & M. Paulino (Eds.), *Police psychology: New trends in forensic psychological science.* Cambridge, Massachusettes: Elsevier Academic Press.

Dalton, G., Milne, R., Hope, L., & Nunan, J. (2018). *"She had ginger hair and horrible teeth" A field study examining how person descriptions are elicited by frontline police officers.* Paper presented at the annual conference of the European Association of Psychology and Law, Turku, June 2018.

Dando, C., Wilcock, R., & Milne, R. (2009). The cognitive interview: Novice police officers' witness/victim interviewing practices. *Psychology, Crime & Law, 15*(8), 679–696. https://doi.org/10.1080/10683160802203963.

Fennell, D. (1988). *Investigation into the King's Cross underground fire*. London: HMSO/Department of Transport.

Gabbert, F., Hope, L., & Fisher, R. P. (2009). Protecting eyewitness evidence: Examining the efficacy of a self-administered interview tool. *Law and Human Behavior, 33*(4), 298–307. https://doi.org/10.1007/s10979-008-9146-8.

Gabbert, F., Hope, L., Fisher, R. P., & Jamieson, K. (2012). Protecting against misleading post-event information with a self-administered interview. *Applied Cognitive Psychology, 26*(4), 568–575. https://doi.org/10.1002/acp.2828.

Gabbert, F., Hope, L., La Rooy, D., McGregor, A., Ellis, T., & Milne, R. (2016). Introducing a PEACE-compliant 'Structured Interview Protocol' to enhance the quality of investigative interviews. In *9th annual conference of the International Investigative Interviewing Research Group (IIIRG)*, London.

Harris, T. (2016). *London's preparedness to respond to a major terrorist incident*. Retrieved from https://www.london.gov.uk/sites/default/files/londons_preparedness_to_respond_to_a_major_terrorist_incident_-_independent_review_oct_2016.pdf

Hope, L., Gabbert, F., Fisher, R. P., & Jamieson, K. (2014). Protecting and enhancing eyewitness memory: The impact of an initial recall attempt on performance in an investigative interview. *Applied Cognitive*

Psychology, 28(3), 304–313. https://doi.org/10.1002/acp.2984.

Jennings, W. G., Fridell, L. A., & Lynch, M. D. (2014). Cops and cameras: Officer perceptions of the use of body-worn cameras in law enforcement. *Journal of Criminal Justice, 42*(6), 549–556. https://doi.org/10.1016/j.jcrimjus.2014.09.008.

Krix, A. C., Sauerland, M., Raymaekers, L. H., Memon, A., Quaedflieg, C. W., & Smeets, T. (2016). Eyewitness evidence obtained with the Self-Administered Interview© is unaffected by stress. *Applied Cognitive Psychology, 30*(1), 103–112. https://doi.org/10.1002/acp.3173.

Leeney, D. G., & Mueller-Johnson, K. (2012). Examining the forensic quality of police call-centre interviews. *Psychology Crime and Law, 18*(7), 669–688. https://doi.org/10.1080/1068316X.2010.534478.

London Fire Brigade. (2017). *EUR evaluation report*. Retrieved from http://www.london-fire.gov.uk/Documents/lfb-evaluation-eur-report.pdf

Mattison, M., Dando, C. J., & Ormerod, T. C. (2018). Drawing the answers: Sketching to support free and probed recall by child witnesses and victims with autism spectrum disorder. *Autism, 22*(2), 181–194. https://doi.org/10.1177/1362361316669088.

Milne, R., & Bull, R. (2006). Interviewing victims of crime, including children and people with intellectual disabilities. In M. R. Kebbell & G. Davies (Eds.), *Practical psychology for forensic investigations and prosecutions* (Vol. 7, No. 24). Chichester: Wiley https://doi.org/10.1002/9780470713389.

Milne, R., & Bull, R. (2016). Witness interviews and crime investigation. In D. Groome & M. Eysenck (Eds.), *An introduction to applied cognitive psychology* (pp. 175–196). Oxford: Routledge.

Myklebust, T., & Alison, L. (2000). The current state of police interviews with children in Norway: How discrepant are they from models based on current issues in memory and communication? *Psychology, Crime and Law, 6*(4), 331–351. https://doi.org/10.1080/10683160008409810.

National Operational Guidance Programme. (2019). *Emergency fire control room operations*. Retrieved from https://www.ukfrs.com/guidance/operations?bundle=control_measure&id=12063&parent=12109

Nunan, J., Milne, R., Shawyer, A., Wakefield, A., Dalton, G., Abbot, R., & Cowup, P. (2016). Don't break the chain: From effective communication to successful decision-making. *Emergency Services Times, 17*(6), 50–52.

Nunan, J., Palfrey-Jones, S., Milne, R., & Wakefield, A. (in press). The timeline of information exchange: An evaluation of London Ambulance Service's front-line communication and emergency response to Exercise Unified Response. *The British Paramedic Journal.*

Risan, P., Binder, P. E., & Milne, R. J. (2016). Emotional intelligence in police interviews – Approach, training and the usefulness of the concept. *Journal of Forensic Psychology Practice, 16*(5), 410–424. https://doi.org/10.1080/15228932.2016.1234143.

Rouse, W. B. (1991). *Design for success: A human-centered approach to designing successful products and systems*. New York: Wiley-Interscience.

Shawyer, A., Milne, R., Dalton, G., May, B., Hope, L., & Gabbert, F. (in preparation). Barriers to communication in the UK Fire and Rescue Service control room. *International Journal of Emergency Management.*

Smith, K., & Milne, B. (2018). Witness interview strategy for critical incidents (WISCI). *Journal of Forensic Practice, 20*(4), 268–278. https://doi.org/10.1108/JFP-03-2018-0007.

Snook, B., Luther, K., Quinlan, H., & Milne, R. (2012). Let'em talk! A field study of police questioning practices of suspects and accused persons. *Criminal Justice and Behavior, 39*(10), 1328–1339. https://doi.org/10.1177/0093854812449216.

van den Heuvel, C., Alison, L., & Power, N. (2013). Coping with uncertainty: Police strategies for resilient decision-making and action implementation. *Cognition, Technology & Work, 16*, 25–45. https://doi.org/10.1007/s10111-012-0241-8.

Waring, D., Alison, A., & Humann, M. (2017, September). *"Ex. Adsorb & Op. Zenith": Information sharing and decision delay in extreme environments*. Paper presented at the meeting of Centre of Research and Evidence on Security Threats conference.

Wright, A. M., & Alison, L. (2004). Questioning sequences in Canadian police interviews: Constructing and confirming the course of events? *Psychology, Crime and Law, 10*(2), 137–154. https://doi.org/10.1080/1068316031000099120.

Further Reading

Bull, R., & Blandon-Gitlin, I. (Eds.). *Handbook of legal and investigative psychology.* London: Routledge.

Griffiths, A., & Milne, R. (Eds.). (2018). *The psychology of criminal investigation; From theory to practice*. London: Routledge.

Marques, P., & Paulino, M. (Eds.). *Police psychology: New trends in forensic psychological science.* Cambridge, Massachusettes: Elsevier Academic Press.

Interviewing Children

Lynne E. Baker-Ward[1] and Gwynn Morris[2]
[1]Department of Psychology, North Carolina State University, Raleigh, NC, USA
[2]Department of Psychology, Meredith College, Raleigh, NC, USA

Keywords
Children · Interviewing · Questioning · Memory

Definition

Interview: A deliberate, structured, interaction in which one individual attempts to obtain needed information from another individual.

Introduction

There are various situations (e.g., disasters, crimes, accidents) in which a first responder's action is urgent and may depend on information only available from a child. This entry is designed to help responders effectively get the information they need from children when it is needed immediately, as well as when the time frame can be extended. As discussed in this article, a productive interview must be tailored to the developmental level of the child. Although individuals beyond late childhood or early adolescence may generally respond to interviewing techniques used with adults, different techniques are required with child interviewees. Further, toddlers, preschoolers, and elementary school students present varying challenges as interviewees and hence require different approaches. But in all circumstances, effective interactions with children require special efforts to minimize their anxiety and gain their trust and cooperation. This process is heavily influenced by the interviewer's approach to the child when they first meet; thus knowing the strategies presented in this chapter in advance contributes significantly to the outcome of the interaction.

This article begins with a review of best practices for the vitally important step of establishing rapport with children of different ages. Next, the discussion advises first responders on how to establish the purpose of the interview for children at different developmental levels. Then, expectations for the provision of information from younger and older children are reviewed. Techniques for obtaining information from interviewees of different ages and in different contexts are then presented, followed by a discussion of considerations when interpreting children's responses.

Establishing Rapport

The first step to a successful interaction with a child of any age is to establish rapport, even when time is of the essence. Good rapport is characterized by comfortable interactions, mutual cooperation, and open communication. Therefore, the primary goal is to help the child develop the trust necessary to provide the needed information. Although more experimental evidence is needed on the contributions of particular components of rapport building, research findings establish that starting an interview by building a good working relationship increases both children's accuracy and completeness in response to subsequent questions (e.g., Price et al. 2016). In short, rapport building should not be skipped, even when limited time is available.

There are several quick and effective adjustments to facilitate rapport (see Teoh and Lamb 2010). For instance, if the child is small, the adult should get down on the child's eye level. The interviewer should convey friendliness through open posture and a warm voice. Toddlers and preschoolers may need to be near an attachment figure (parent or other loved one) or to hold an attachment object (favorite toy or blanket) to feel safe and secure. Toddlers often fear strangers, so the interviewer should not initiate touch but rather give the child as much control as is possible. Crying children do not benefit from criticism or invalidation of their feelings. A better response to crying is a sincere "I know why you are upset and I'm here to help." Additionally, when children get loud, using a calm, soft voice may entice them to stop yelling or crying so they can hear what is being said to them. The physical comfort of the child also needs to be attended to. Toddlers and young preschoolers lack an awareness that adults do not know everything that they know, so these young children may mistakenly assume that adults are aware of their physical injuries and fail to point them out. Lastly, for children of all ages, interviewers should calmly and clearly assure the child that they are there to help and introduce themselves in simple, direct language; "I'm Officer Smith and I will help you."

In situations where more time and resources are available to devote to rapport building, there are several additional techniques that are effective. If possible, the child should be given a choice of who they would like to talk to. Some children connect better with people who look like them, are of a specific gender, or remind them of a trusted adult. For children of preschool and elementary ages, adults should start with a warm-up conversation about a non-threatening topic such as a recent event (holiday celebration, birthday party, family gathering) or hobby (sports, music, school topics). Results are best when adults pose invitations for an open-ended response (i.e., "Tell me all about your last birthday") rather than directive questions that dictate a specific kind of response (i.e., "Where was your last birthday party?") (Price et al. 2016). Adults should keep in mind that younger children's attention spans are much shorter than older children's, and thus the length of these warm-up conversations should be brief. Furthermore, responders should keep the continual physical comfort of the child in mind as the interactions proceed. Young children need to be explicitly told that they can take a break and they should not be expected to sit still for long periods of time. As long as the child is engaged in the interview, the responder should tolerate fidgeting, walking around, playing with toys, etc. Responders can redirect the child's attention as needed using simple and direct statements, e.g., "I cannot hear you when you are under the table. Please sit in the chair. We need to do more talking."

Conveying Purpose

After rapport has been established, the interviewer needs to clearly convey their purpose for talking with the child and the child's role as an informant, practices which appear to help children be more informative (Teoh and Lamb 2010). A word of caution here: *Interviewers should limit their questions to only topics that are essential for them to do their current job. If the purpose of the questions is to gather evidence for criminal or civil court and is not urgent (*i.e., *sexual abuse victim, custodial investigation), STOP!* Poor questioning techniques can contaminate a child's memory, making their future testimony suspect. However, well-trained child forensic investigators can elicit valuable information from children. Evidence shows that it takes many hours of intensive training with detailed feedback on techniques to master standard child interview protocols (Lamb 2016). In short, if the information needed from a child will have serious legal consequences, call in a trained child forensic psychologist as soon as possible.

When time is urgent, a clear, simple statement of the emergency responder's purpose will suffice. For instance, "I need to make sure everyone is out of the building" or "I will help you find the grown-ups you came with." Responders should use "I" language and address only the immediate purpose.

In situations where the responder is not rushed, the responder may need to reassure the child that the child is not in trouble. Preschoolers and young elementary children will benefit from an invitation to share in the responder's purpose: "You can be a helper." Due to preschoolers' egocentrism, they need to be explicitly told that they know more than the interviewer and that it is ok to tell the responder if the responder is wrong. Preschoolers and elementary-aged children should be clearly instructed about the "interview rules." That is, children should be told to tell the truth, say "I don't know" rather than making up an answer, and to correct the interviewer if they make a mistake. Then, children can be given practice using the rules. The interviewer could say, "What did you have for breakfast? What did I have for breakfast?" Ensure that children respond that they do not know what the interviewer had for breakfast.

Understanding Age-Related Changes

The information children can provide depends both on age and the types of questions directed toward them. Although infants can recognize information – e.g., can hear a voice and know that it is familiar – the capacity to remember and

report personal experiences typically emerges in the toddler years. It was once assumed that children could not remember their experiences until they were about 4. It is the case that adults have difficulty retrieving memories for events that occurred before this age, a phenomenon described as childhood amnesia. However, it is now well established that many 2-year-olds can provide accurate responses to specific questions about their recent past experiences (Fivush 2011).

Clear developmental improvements are apparent in underlying memory capacities. Three-year-olds often can provide some information about past events in response to general questions (e.g., "Tell me about the accident"), although the amount of information they provide is still limited and does not typically include a great deal of detail. Older preschoolers and kindergarteners provide more extensive reports of their experiences in response to general, open-ended questions and with age, provide increasingly complete accounts, including descriptive details. By about age 7, young interviewees rely much less on the interviewer's specific questions and can provide rich, independent narrative accounts of some types of events. By the end of the elementary school years, most children have the memory capability to report events in an adult-like manner, often including information about time and place, the chronology of the event, and even some detail about emotions and thoughts (Reese et al. 2011).

Memory depends on a variety of influences in addition to age. Children's reports may exceed expectations for their age level when they have a great deal of knowledge regarding an event (see Baker-Ward et al. 2009). In this case, they may take in more information about an experience and retain it over longer intervals than is the case when they are asked to report events they do not fully understand. For example, a child who is an avid baseball fan will likely report a variety of actions and details ("It was during the third inning when the team's pinch hitter took bat") than a less enthusiastic peer can recall ("Sometime after the game started. . .").

The nature of the to-be-remembered event also impacts the child's subsequent report of that event. The anxiety experienced by the interviewee as an event transpires is of particular relevance to first responders. The existing evidence, however, does not support straightforward conclusions about the relationship between stress as an event is experienced and subsequent memory for the experience. It appears that stress affects what the individual focuses on during the event, a process that is affected by a child's developmental level and other factors (Quas et al. 2014). Of course, if actions or descriptions are not taken into memory, they cannot be reported. Notably, the "weapon focus effect" involves an individual's focus on sources of danger, limiting the attention they can direct to other aspects of the experience (Fawcett et al. 2016). Thus, responders should accept that a child may not have available in memory some apparently obvious information about an anxiety-provoking event. This limitation notwithstanding, it is clear that children can provide a great deal of information about stressful experiences and that supportive interviewing reduces suggestibility (Quas et al. 2014).

Regardless of the age of the individual and the type of event, memory is subject to change over time. In addition to loss of information as time goes by, the content of memory can be altered by experiences that transpire after the initial occurrence of the event. Memory is sometimes erroneously presented as functioning as a video recorder, resulting in an exact copy of an event. However, in actuality, memory is a dynamic process, with events often reconstructed as knowledge changes (Baker-Ward et al. 2009). It should be emphasized that such constructive processing is different from intentional lying in that individuals are reporting events as they understand them. For instance, when adults omit very salient details from an initial event report and include them only later, the inconsistency in their reports may indicate lying. In contrast, a child's provision of additional detail over time often simply reflects growth in the understanding of what listeners may want to know. Similarly, a child who initially describes a car as "a race car" may later report that it was a "BMW." Furthermore, toddlers and preschoolers tend to report information in a piecemeal fashion, sometimes adding important new details even after they indicate "that's all I can remember."

Children, especially those younger than early elementary school age, may even remember new details at a later interview. This inconsistency is developmentally normal and generally doesn't contradict information initially reported but rather augments it. So while an adult's omission of the fact that the man he saw was over 7 ft tall would be suspect, a child's provision of the fact that the man was "really, really tall" a few days later would not be unusual among preschoolers (Brubacher et al. 2019).

Obtaining Information from Children

In talking with children, an effective interviewer provides just enough guidance and direction to enable a child to participate fully in the exchange of information. The adult's contributions, in effect, compensate for the child's developmental limitations. This approach is an example of the technique psychologists describe as scaffolding. In the interview context, the responder scaffolds the child's involvement by providing structure and insuring that the child understands the interviewer's questions. In doing so, the interviewer bridges the gap between the child's level of cognitive and language development and the skills needed to effectively convey extensive and accurate information. Consequently, the child's interview performance exceeds the level of competence the child could demonstrate without such scaffolding. Further, the child's current skills determine the amount of appropriate scaffolding that is required, and generally younger children need more guidance than older children. Note that the interviewer is supporting the child's own contributions to the interview, rather than fully controlling the interaction.

Effective interviewers must accommodate the child's level of language development. The child's acquisition of language involves more than simply growth in vocabulary. Toddlers and preschoolers are especially likely to overextend the meaning of words to cover whole categories and to incorporate related objects. For instance, "yesterday" often means "any time in the past" to toddlers. Furthermore, a younger preschooler may call a zebra a horse or a teenager a man.

Similarly, younger children may also limit a category much more severely than would be the case with adults. A child carrying a stuffed animal may report that he didn't have a toy with him, because the stuffed animal is his "lovey," which he sees as its own category. Interviewers must also keep in mind age-related changes in the child's capacity to understand grammatical structures and conventions of conversations (as discussed below).

In general, in situations in which the need for information is not urgent, hierarchically structured interviews result in the most complete and accurate account of the child's experience. Hierarchically structured interviews move from the most general prompts to increasingly specific requests for information to obtain the child's complete account of the event.

In some circumstances, the responders need immediate information in order to take emergency action ("Who is in the house right now?"). In such situations, applying the full hierarchical interview structure would require time that isn't available. In these cases, the emergency responder should skip the open-ended section and instead immediately present wh-questions to obtain the needed information as quickly as possible. In most cases, beginning with more focused questions is also appropriate for working with young toddlers.

Open-Ended Prompts. Following the establishment of rapport and a child-friendly discussion of the purpose of the interview, the hierarchical interview begins with open-ended prompts, which are general questions and statements by an interviewer that do not direct the respondents' attention to a specific component of an experience.

For example, "Tell me what happened when Mommy got hurt." As needed, the interviewer follows up with non-specific probes to obtain additional information, e.g., "Tell me more about that," or "What else do you remember?" This practice avoids introducing incorrect information that could contaminate a child's later report and, indeed in some instances, the child's memory for the event.

To support the child's continued engagement in the interview, the respondent should provide

ongoing, positive feedback by simply acknowledging the child's response. For example, the interviewer may say, "uh huh," or "ok." These simple reactions indicate to children that it is their turn to talk. Although the child may require praise to continue talking, interviewers must be very careful to avoid reinforcing a particular answer or response. To maintain the child's engagement without the risk of altering a report, it is best to use phrases like "You're doing a good job," or "Thank you for talking with me." It is important to avoid linking praise and specific answers because young children typically want to please adults. Thus, they may alter their reports to provide information that they assume will elicit praise. Because children often see adults as authority figures, they are sensitive to the interviewer's reactions to their answers.

Focused Prompts. Once the child is no longer providing new information in response to open-ended prompts, the responder may move on to the next phase of the hierarchical interview by presenting focused prompts. These more targeted requests for information are questions and statements by an interviewer that direct the respondent's attention to a specific component of an experience. These include the use of who, what, when, and where questions as well as yes/no questions.

The interviewer should craft wh-prompts using details a child has already provided; e.g., "You said the car didn't start. Where was the car when it didn't start?" Questions asking who, what, when, or where tend to elicit more useful information than yes/no probes (Stolzenberg and Lyon 2017). Such wh-prompts target a particular fact without feeding the child the answer, as is the case with yes/no questions. Further, wh-questions generally avoid providing the child with information that could be incorporated into subsequent reports of the event, risking contamination of the child's memory.

Effective wh-prompts, however, require careful phrasing. Children younger than about 7–8 have difficulty with how and why questions, which should be avoided. Responding to these questions typically requires an understanding of causal relations and inferring others' perspectives and motivations, which are usually beyond the cognitive capabilities of young children (Malloy et al. 2017). Similarly, younger children have difficulty with abstract concepts such as clock and calendar time. It is always advisable to scaffold children's reporting of the time of the event by linking it to regular occurrences in the child's day (e.g., "Was that before your mom got home from work?") or landmark events ("Was that after you started kindergarten?"). In addition, the interviewer should remain aware of differences in children's and adults' understanding of the world, in order to avoid limiting the child's responses. For instance, in response to an interviewer's question about what a child had for lunch, a 3-year-old reported that his babysitter did not give him lunch. Follow-up questioning determined that the child's caregiver had given him eggs for lunch, which he did not consider to be lunch because "eggs are for breakfast." Any questions about his babysitter's care were alleviated when the child was asked to tell the interviewer everything he had to eat at the caregiver's house. This example also illustrates the importance of follow-up questions to maximize the information that can be reported in response to the prompt.

If a child does not know the information that a responder needs, a little creativity may help. For instance, a toddler may answer "What is your mom's name?" with "Mommy" but may provide her name in response to "What does your Grandma call your Mommy?." Similarly, if a young child cannot tell their address or phone number, they may be able to name their school or daycare, and a call to such facilities may yield the information.

In addition to the importance of phrasing questions that are sensitive to the child's understanding of the meaning of words and knowledge of the world, interviewers should also be aware of developmental limitations in interpreting word order. All interviewees, especially children, will benefit from short, direct questions. Such questions require less working memory and minimize the steps required to comprehend the interviewer's request. Table 1 below lists several specific recommendations for presenting appropriate questions to child interviewees. As indicated in the

Interviewing Children, Table 1 Practices for interviewing children

Dos	Don'ts
Start the interview with open-ended prompts Example: "Tell me what happened."	Immediately jump to specific wh- or yes/no questions when there is time to obtain a child's full report Examples: "Who started the fire?" "Did your Mom start the fire?"
Use who, what, when, and where questions Example: "What happened when your Mom drove off the road?"	Use questions that ask about how or why Example: "Why did your Mom drive off the road?"
Use follow-up questions to understand the meaning of a child's statements Example: *Child:* "Emma is still in the burning house!" *Interviewer:* "Who is Emma?" *Child:* "My goldfish."	Make assumptions about a child's intent or understanding Example: *Child:* "Emma is in the burning house!" *Interviewer assumes Emma is a person.*
Use questions that prompt with actions or observational-based cues the child has already provided Example: "What happened after the car slid off the road?"	Use questions that prompt with time-based cues Example: "What happened last night?"
Scaffold a child's report about time Example: "Was that before lunch?"	Use questions about clock or calendar time Example: Was that around 3 pm?
Use the active voice Example: "Where did the man hide?"	Use passive voice Example: "Where was the man hiding?"
Ask one question at a time Example: "Who was there?"	Use multipart questions Example: "Who was there and what did they say?"
Use simple, direct prompts Example: "Tell me who did it."	Use tag questions Example: "You know who did it, don't you?"
Reference actual behaviors or events Example: "Where does your mom usually go?"	Reference hypothetical events Example: "What if I was your Mom...where would I be?"
Instruct children to respond Example: "Tell me about . . ."	Use indirect requests Example: "Do you want to tell me about that?"
Have a child point on their own body or use actual photos of a location Example: "Show me on your body where the man hit you." Example: "Here are some pictures of the park. Show me where the car was parked."	Use toys as props to reenact an event Example: "Show me on this doll where the man hit your Mom." Example: "Point on the map to where you last saw the car."

table, the passive voice, multipart questions, and tag questions should be avoided.

Props. When verbal information from a child is not forthcoming, interviewers are often drawn to the use of dolls or other props (for review, see Poole and Bruck 2012). Although it seems reasonable to offer the option of a nonverbal response in this situation, the practice is problematic, especially for toddlers and preschoolers. These young children have difficulty in seeing a doll both as a representation of the self and as a toy; consequently, dolls are not effective as interview aids for this age group. Because the practice does not elicit reliable information, it should be used only as a last resort and then with the understanding that evidence obtained in this manner is generally suspect. Similar concerns apply to the use of body diagrams. It is also intuitively appealing to allow children with limited verbal skills to act out the events under discussion, using a variety of props. Although young children may generate some additional information using props, they also become distracted by the situation and play with interview aids in a manner that results in false evidence. Further, research shows that older children do not generate additional evidence with dolls and props. So, younger children don't benefit from such interview aids, while older children don't need them.

Although toys are not effective interview aids, more realistic objects may be useful in obtaining information from younger children in some circumstances. They may be able to indicate on their own bodies (cf. on doll) where an injury occurred. Similarly, when information about a location is necessary and is not reported verbally after sensitive questioning, the use of an accurate photograph (in contrasts to a map) in the investigative phase may assist the child in identifying a location. Nonetheless, such techniques should be used only when attempts to obtain the information verbally have not proven successful.

Interpreting Children's Responses

The best rule of thumb for interpreting young children's response is to assume they are telling the truth but to remember that children's truth reflects their perceptions of the world. Concocting a believable lie involves cognitive skills that exceed the developmental capabilities of toddlers and young preschoolers. Lying – that is, constructing a false story in order to manipulate someone else's understanding of events – requires a number of abilities that are not generally well established until the early elementary school years. These capabilities involve the complicated understanding of how minds work, including knowing that thoughts are private and can differ among people; taking the perspective of another person; and attributing motives and intentions to others. It is certainly the case that young children may falsely deny actions in response to yes/no questions or direct probes. For example, a 4-year-old child whose face is covered with sprinkles and powdered sugar may say "No!" when asked "Did you eat my doughnut?" or say "It was the dog!" in response to "Who ate the doughnut?". These simplistic false reports, provided in order to avoid punishment, differ from a spontaneous narrative about an event. It would be a rare preschooler who would provide a detailed description of the dog's eating the doughnut without being asked specific questions about the missing pastry (for review, see Talwar and Crossman 2012).

To argue that young children do not concoct sophisticated lies as part of a scheme does not imply that all their statements would correspond to an adults' version of what happened. Especially given their limitations in understanding cause and effect and intent, a child may provide a report that does not reflect what actually transpired. For example, a 3-year-old boy asked to describe what happened during a visit to the doctor said that "The nurse put blood in my finger!" in attempting to report the nurse's obtaining a drop of blood to check his hemoglobin. Such limitations are especially relevant in situations in which the task involves differentiating intentional and accidental injuries. To illustrate with a mundane experience, a preschooler who reports that "Mommy hurt me!" may reference a situation in which the mother unintentionally clipped the child's nail too closely. Thus, it is important for an interviewer to be mindful of assumptions made from an adult's worldview. It is very important to clarify children's meanings with carefully selected follow-up questions, as discussed above.

Of course, not even the most carefully constructed follow-up questions can resolve all ambiguity. Identifying the source of information in memory is challenging for children as well as adults. Most children have difficulty, for example, in remembering whether their teacher or their neighbor told them about an upcoming event, although they may report in detail what they heard in the conversation. Misremembering the source of the information is a common error and in no way indicates that the information itself is inaccurate (Brubacher et al. 2019).

It is also the case that the credibility of a child's report cannot be assessed using the standard applied to adults. As indicated above, children may provide only a few pieces of information spontaneously, may not elaborate their responses, and may give their account in a piecemeal fashion. However, experimental evidence (Gordon and Follmer 1994) indicates children give accurate information in response to open-ended questions even when the information is limited and may introduce salient details later in an interview without contradicting the earlier report.

One final point of emphasis is the importance of documenting the child's report as completely and accurately as possible as soon as time permits, especially if an ongoing investigation is likely. Documenting the child's report involves reporting as much of the interview as possible, including the procedure used to establish rapport, the interviewer's actual questions, the child's verbal and nonverbal responses, and any additional information that could help later interpret the child's account.

Conclusion

Getting useful information from children is not easy. It requires sensitivity, patience, and skill on the part of the responder. But learning and using best interview practices is well worth the effort. With effective scaffolding from adults, even young preschoolers can provide answers that can determine the success of an emergency action or influence the outcome of a forensic proceeding.

Cross-References

- ▶ Emergency Management: Working with Vulnerable Populations
- ▶ Interviewing Adults: Communication at the Front Line
- ▶ Investigations: Accidents and Reconstructions
- ▶ Investigations: Criminal

References

Baker-Ward, L., Ornstein, P. A., & Starnes, L. P. (2009). Children's understanding and remembering of stressful experiences. In J. Quas & R. Fivush (Eds.), *Emotion and memory in development: Biological, cognitive and social considerations* (Series in Affective Science, pp. 28–59). New York: Oxford University. https://doi.org/10.1093/acprof:oso/9780195326932.003.0002.

Brubacher, S. P., Peterson, C., La Rooy, D., Dickinson, J. J., & Poole, D. A. (2019). How children talk about events: Implications for eliciting and analyzing eyewitness reports. *Developmental Review, 51*, 70–89. https://doi.org/10.1016/j.dr.2018.12.003.

Fawcett, J. M., Peace, K. A., & Greve, A. (2016). Looking down the barrel of a gun: What do we know about the weapon focus effect? *Journal of Applied Research in Memory and Cognition, 5*(3), 257–263. https://doi.org/10.1016/j.jarmac.2016.07.005.

Fivush, R. (2011). The development of autobiographical memory. *Annual Review of Psychology, 62*, 559–582. https://doi.org/10.1146/annurev.psych.121208.131702.

Gordon, B. N., & Follmer, A. (1994). Developmental issues in judging the credibility of children's testimony. *Journal of Clinical Child Psychology, 23*, 283–294. http://doi.org/10.1207/s15374424jccp2303_6

Lamb, M. E. (2016). Difficulties translating research on forensic interview practices to practitioners: Finding water, leading horses, but can we get them to drink? *American Psychologist, 71*(8), 710–718. https://doi.org/10.1037/amp0000039.

Malloy, L. C., Orbach, Y., Lamb, M. E., & Walker, A. G. (2017). "How" and "Why" prompts in forensic investigative interviews with preschool children. *Applied Developmental Science, 21*(1), 58–66. https://doi.org/10.1080/10888691.2016.1158652.

Poole, D. A., & Bruck, M. (2012). Divining testimony? The impact of interviewing props on children's reports of touching. *Developmental Review, 32*, 165–180. https://doi.org/10.1016/j.dr.2012.06.007.

Price, E. A., Ahern, E. C., & Lamb, M. E. (2016). Rapport-building in investigative interviews of alleged child sexual abuse victims. *Applied Cognitive Psychology, 30*(5), 743–749. https://doi.org/10.1002/acp.3249.

Quas, J. A., Rush, E. B., Yim, I. S., & Nikolayev, M. (2014). Effects of stress on memory in children and adolescents: Testing causal connections. *Memory, 22*, 616–632. https://doi.org/10.1080/09658211.2013.809766.

Reese, E., Haden, C. A., Baker-Ward, L., Bauer, P. A., Fivush, R., & Ornstein, P. (2011). Coherence of personal narratives across the lifespan: A multidimensional model and coding method. *Journal of Cognition and Development, 12*(4), 424–462. https://doi.org/10.1080/15248372.2011.587854.

Stolzenberg, S. N., & Lyon, T. D. (2017). 'Where were your clothes?' Eliciting descriptions of clothing placement from children alleging sexual abuse in criminal trials and forensic interviews. *Legal and Criminological Psychology, 22*, 197–212. https://doi.org/10.1111/lcrp.12094.

Talwar, V., & Crossman, A. M. (2012). Children's lies and their detection: Implications for child witness testimony. *Developmental Review, 4*, 337–359. https://doi.org/10.1016/j.dr.2012.06.004.

Teoh, Y.-S., & Lamb, M. (2010). Preparing children for investigative interviews: Rapport-building, instruction, and evaluation. *Applied Developmental Science, 14*, 154–163. https://doi.org/10.1080/10888691.2010.494463.

I

Further Reading

Lamb, M. E., Orbach, Y., Warren, A. R., Esplin, P. W., & Hershkowitz, I. (2007). Enhancing performance: Factors affecting the informativeness of young witnesses. In M. P. Toglia, J. D. Read, D. F. Ross, & R. C. L. Lindsay (Eds.), *The handbook of eyewitness psychology, Vol. I: Memory for events* (pp. 429–451). Mahwah: Lawrence Erlbaum Associates Publishers.

Lyon, T. D. (2014). Interviewing children. *Annual Review of Law and Social Science, 10*, 73–89. https://doi.org/10.1146/annurev-lawsocsci-110413-030913.

Poole, D. A. (2016). *Interviewing children: The science of conversation in forensic contexts*. Washington, DC: American Psychological Association. https://doi.org/10.1037/14941-000.

Intrusion Detection Systems

David J. Brooks and Michael P. Coole
Security Science, School of Science, Edith Cowan University, Perth, WA, Australia

Keywords

Alarm system · Threat · Risk · Defense in depth · Sensor · Geometry

Definition

An Intruder Detection System (IDS) is an automated technology designed and implemented to detect and communicate the presence of a person or object in a designated zone. IDS provides the *detection* element in a security system which holistically deters, detects, delays, and responds.

Introduction

Intrusion Detection Systems (IDS) have become a protection norm in both domestic and commercial premises, driven by cost reductions, a user-pay approach to security, and an increased perceived need (Brooks 2014). Such a need is driven in part by burglary risks, a "high-volume crime that impacts upon the well-being of the general public" (Mawby 2007). While no IDS can physically prevent a theft, they do notify of such activity. As a result, IDS have become a common method of protection. Therefore, this entry introduces IDS, its principle and geometry of detection, taxonomies of sensing detectors, and applied levels of protection.

What Is an Intrusion Detection System?

IDS have many different names. ASIS International refers to these systems as *Intrusion Detection Systems* (Walsh and Healy 2012, p. 91), whereas in Australia, they are *Intruder Alarm Systems* (Standards Australia 2007). Other terms to describe IDS include Burglar Alarms, Alarm Systems or simply, Alarms. IDS is also a commonly used term within cybersecurity, being a device or software that monitors a computer network for malicious or policy violations (Abaimov and Martellini 2017, p. 31). Nevertheless, for this entry, IDS is an element of a physical security system designed to detect and communicate the presence, entry, or attempted entry of an unauthorized intrusion activity into a designated zone.

The security literature considers IDS as a dichotomy between domestic and commercial; however, there is little difference in their principles, design, and, to some degree, application. Factors that do define these systems are the diagnosed threats and risks that drive the inferred robustness of the IDS as a treatment strategy to detect threats.

Defense in Depth

The function of IDS is to support the Defense in Depth strategy. Defense in Depth protects people, information, or assets through the elements of *deter*, *detect*, *delay,* and *response* (Garcia 2008, p. 58). In the security system, IDS both *deters* and *detects* a person or object of interest.

Detection of overt or covert movement must be accomplished to prevent loss or harm, achieved through a variety of sensing detectors. Therefore, detection is a critical function of the Defense in Depth strategy, as without detection it is only a matter of time before an intruder penetrates

all barriers (delay) to reach their desired asset. Effective security is related to time after detection; therefore, timely detection is required to facilitate apprehension (Garcia 2008).

Principle of Intrusion Detection

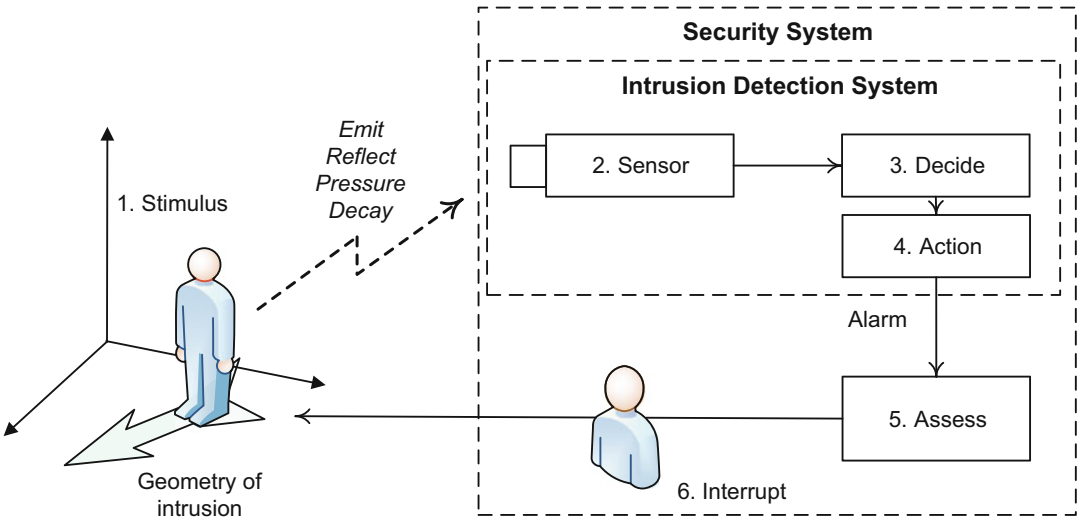
The principle of detection relies on the use of sensing technology to discover and respond to the presence of a person or object within a defined field of view. All automated systems comprise sensing, processing (decide), and output (action) componentry. Figure 1 schematically highlights how an IDS senses the presence or activities of a person or object in response to anomalous activity.

- *Stimulus* (1) is introduced by the presence of a person or object. Stimulus could be emitted energy such as infrared radiation, a reflected wave such as microwave radiation, a pressure wave, or molecular decay.
- The *sensor* (2) reacts to a compatible *stimulus*. There is a wide range of sensing detectors, ranging from a *passive infrared* detector seeking emitted infrared radiation, *break-glass* detector tuned to the frequency of breaking glass to an *active microwave* detector that receives a Doppler shifted wave.
- An algorithm *decides* (3), based on a priori threshold, whether to *act* (4) in producing an alarm which indicates an anomalous stimulus has been detected.
- A person or thing *assesses* (5) the alarm to judge and, if appropriate, initiate a human response to *interrupt* (6) the person or object.

These events demonstrate that the process of intrusion detection is not an instantaneous event, nor a guaranteed outcome.

Geometry of Intrusion Detection

Detect is the discovery, through sensing a stimulus, of a person or object. IDS detection is achieved through the geometry of protection (Underwood 1984), which highlights an intruder can be detected through crossing a line, moving through an open space, or contacting a specific point accordant with an intrusion geometry. The aim of employing sensors across this geometry is to achieve what Garcia (2008) and Wyss (2009) term "balanced protection," where every viable intruder scenario pathway achieves the same level of difficulty. For spatial detection,



Intrusion Detection Systems, Fig. 1 The principle of detection. (Adjusted from Brooks 2014, p. 687)

the stimulus may move into a sensing detector's field of view from many directions, horizontally and/or vertically. Furthermore, the stimulus may move fast or slow, be large or small, be close or far from the detector, or have a different chemical make-up. Such vector movement can be considered the geometry of intrusion, articulated by the designated alarm zone.

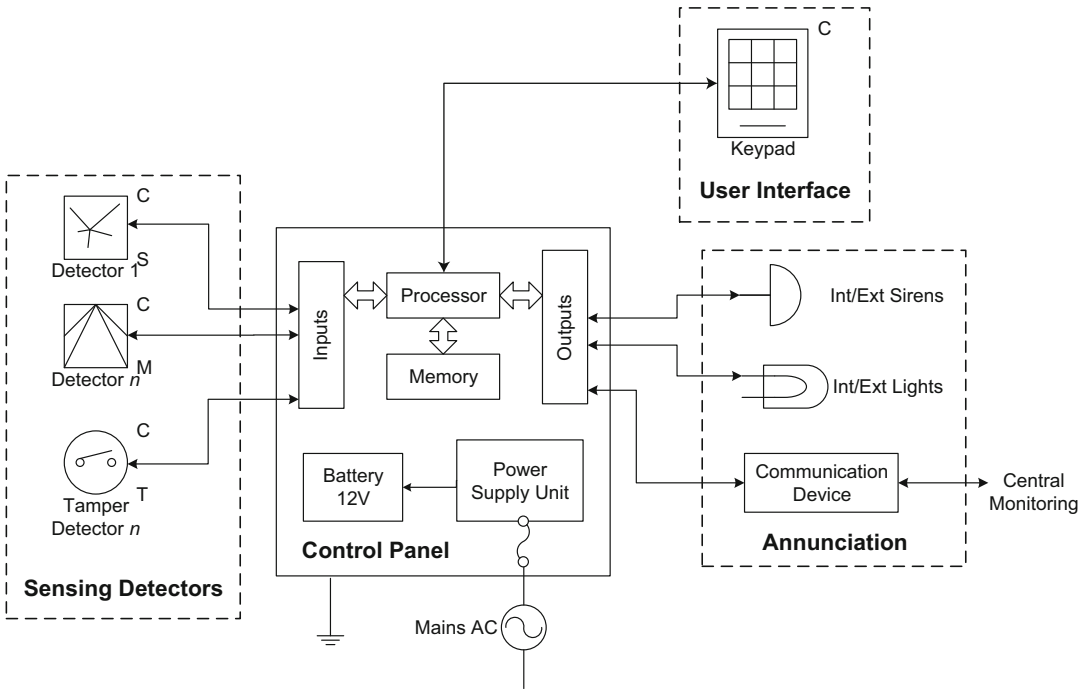
A sensing detector must be designed and applied to maximize its strength based on its underlying physics sensing principle while minimizing its inherent weakness. For example, a passive infrared detector most effectively senses targets moving *across* its field of view at an ideal distance and speed within a temperature threshold.

Sensing detectors can be defeated through a variety of methods, such as bypass, spoofing, or technical defeat. Bypass may include going over, under, or around the detector's field of view. Spoofing is defeating the detector by moving through its field of view without stimulating the sensor above its activation threshold. Technical defeat is the ability to modify the input or output function of the IDS. The ability to successfully defeat a detector requires both capability and knowledge of the detector, the IDS, and its applied environment.

Taxonomy of Sensing Detectors

The sensing detector is often not considered the primary element of the IDS; instead, the focus is the Control Panel (see Fig. 2). Nevertheless, there are different taxonomies in the categorization of detectors. For example, Smith and Brooks suggest that "detection technologies can be categorised as single or many-dimensional" (2013, p. 141) or in accordance to Underwood, by their geometry of protection (1984, p. 137). Nevertheless, taxonomy can best be presented in accordance to detection geometry (Table 1).

In contrast, Garcia's (2008) classification of detectors employs an *application* taxonomy with passive or active, covert or visible, line-of-



Intrusion Detection Systems, Fig. 2 Typical IDS. (Brooks 2014, p. 689, reproduced with permission of Palgrave Macmillan)

Intrusion Detection Systems, Table 1 Geometric taxonomy of sensing detectors

Detection	Geometry	Example
Point	0	Operates at a zero-dimensional point. Examples are door reed switches and micro-switches
Line	1	Operates as a dimensional line. Examples are active infrared photoelectric beams or optic fiber cables along walls or fences
Wall or blanket	2	Operates in the vertical and horizontal dimensions. Examples are vibration detector on walls or active stacked infrared photoelectric beams
Volumetric	3	Operates within a region of dimensional space. Examples are microwave, ultrasonic, and passive infrared detectors
Volumetric and time	4	Operates within a region of dimensional space and time. Examples are surveillance system with a record and replay function

Adjusted from Smith and Brooks 2013, pp. 141–142

Intrusion Detection Systems, Table 2 Applied IDS security

Applied security	Sensing geometry	External alarm	Anti-tamper	Communication line monitor	Central monitor
Low threat	Single point	No	No	No	No
⇕	Volumetric	Maybe	Yes	2-state	Maybe
⇕	Multipoint	Yes	Yes	3-state, including unarmed	Yes
High threat	Multipoint and overlapping fields	Yes	Yes	4-state, with fault and tamper	Yes
	Multipoint, overlapping, and hierarchical logic	Yes	Yes	Active encryption	Yes

Adjusted from Brooks 2014, p. 690

sight or terrain-following, volumetric or line detection, and application. Finally, detectors can also be categorized by the sensors underlying physics of operation such as radio, microwave, infrared, or x-ray.

Elements of an Intrusion Detection System

A typical IDS is a system that integrates discrete sub-systems or components (Fig. 2). The Control Panel comprises a central processor, memory, input and output interfaces, power supply, and battery back-up. Detectors will comprise of various types of sensors. A User Interface, such as a keypad, allows users to interact with the IDS. Finally, Annunciator may include external and internal audible warning devices and lights and, for an off-site monitored system, some form of external communication.

Levels of Applied Detection

From an application context, as threats and risks increase, so should the capability of the IDS (Table 2). With a lower threat, an IDS may only require point detectors and local alarm annunciation. As threats escalate, the degree of protection should be commensurate to not only the detection but also unauthorized tamper attempts. For example, two detectors that have overlapping fields of views to increase the probability of detection, hierarchical detectors that apply an OR logic, the use of detectors on enclosures (anti-tamper) to sense access, and that communications lines are supervised to mitigate bypass. Tamper resistance

is important as this is the capability of the IDS to withstand an internal covert attack.

Conclusion

Intrusion Detection Systems have become commonplace within our built environment, used as a situational crime prevention strategy to target hardens. Thus, the application of these systems supports the security principle of Defense in Depth through their ability to sense intrusion and initiate a response, increasing the risk to offenders and altering behavior. The ability to detect is achieved through the detector's sensor, which reacts to a defined stimulus such as a person or object within a field of view or detection zone. Nevertheless, the ability of a sensor to achieve efficacy in detection is achieved through the likely geometry of intrusion, as well as the greater security system.

Cross-References

- ▶ Insider Threat
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Interior Applications
- ▶ Physical Security: Methods and Practices
- ▶ Security: Theories

References

Abaimov, S., & Martellini, M. (2017). Selected issues of cyber security practices in CBRNeCy critical infrastructure. In M. Maurizio & A. Malizia (Eds.), *Cyber and chemical, biological, radiological, nuclear, explosives challenges: Threats and counter efforts*. Cham: Springer.

Brooks, D. J. (2014). Intrusion detection systems in the protection of assets. In M. Gill (Ed.), *The handbook of security* (2nd ed., pp. 683–704). Basingstoke: Palgrave Macmillan.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Burlington: Butterworth-Heinemann.

Mawby, R. I. (Ed.). (2007). *Burglary*. Aldershot: Ashgate Publishing Group.

Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*. Waltham, MA: Elsevier.

Standards Australia. (2007). *AS/NZS 2201 intruder alarm systems – Part 1: Client's premises-design, installation, commissioning and maintenance*. Sydney: Standards Australia.

Underwood, G. (1984). *The security of buildings*. London: Butterworths.

Walsh, T. J., & Healy, R. J. (2012). *Protection of assets*. Alexandria: ASIS International.

Wyss, G. D. (2009). *Quantifying the degree of balance in physical protection systems*. Albuquerque: Sandia National Laboratories.

Further Reading

Brooks, D. J. (2014). Intrusion detection systems in the protection of assets. In M. Gill (Ed.), *The handbook of security* (2nd ed., pp. 683–704). Basingstoke: Palgrave Macmillan.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Burlington: Butterworth-Heinemann.

Smith, C. L., & Brooks, D. J. (2013). Chapter 6 detection systems. In *Security science: The theory and practice of security* (pp. 129–152). Burlington: Butterworth-Heinemann.

Investigations: Accidents and Reconstructions

E. Parrott
Liverpool John Moores University, Liverpool, UK

Keywords

3D modelling · Photogrammetry · Laser scanning · Photography · Crime scene · Reconstruction · Mass disaster · Structure from motion

Definition

Reconstruction is the combined process of applying scientific methods, physical evidence, and reasoning, to determine the most probable sequence of events that occurred during an incident or the commission of a crime (ACSR 2019).

Introduction

This entry explores the process of scene reconstruction focusing upon the scientific methods, technologies, and apparatus used when reconstructing small and large-scale incidents. The purpose of reconstruction is to aid investigators in determining what happened and how it occurred through the examination and analysis of preserved incident sites, recorded digitally and/or physically using scientific methods (Chisum and Turvey 2011). Over the last decade, there has been a proliferation of reconstruction technologies and methods (see entry ►"Drones") which have benefitted law enforcement practice worldwide. Not only in the handling of criminal investigations but also in the management and assessment of incidents resulting from acts of war or terrorism as well as accidents and natural disasters.

Generally in the criminal realm, shootings, homicides (Buck et al. 2013), and road-traffic accidents (Buck et al. 2007) have been the primary focus of reconstruction efforts over recent years. This is due to their complexity and the increasing involvement of specialists such as collision engineers in the case of road traffic accidents, or blood pattern analysis (BPA) experts and ballistics specialists in the case of shootings and homicides (Houck et al. 2018). As such, the consultation of these experts and others has also become commonplace when reconstructing substantially larger mass incidents and emergency scenarios, such as plane crashes, explosions, acts of terrorism, and fire investigations. As due to the mechanic nature of these incidents, investigators can determine whether the acts may have been criminal or accidental, such as in the case of plane crashes where the positioning of debris can indicate the site of impact (AAIB 2017). In addition to this, understanding of the mechanism by which the incident occurred may also prove valuable to manufacturers or policy makers to limit the possibility of future occurrence.

With regard to this, unlike many of the other tasks carried out by law enforcement, mass disaster incidents demand heightened multi-agency cooperation to manage the safety of the public and practitioners over potentially large areas, as well as taking care to record, process and package any evidence likely to determine the cause of the event. As such, reconstruction is becoming an increasingly valuable tool, providing investigators with new insights from new perspectives to support more efficient practices. In addition to this, the results of these large-scale reconstructions are also valuable to local government, utility providers, and engineers to facilitate recovery of the area, as well as aiding future law enforcement training to inform procedures and practice worldwide.

However, despite improved capture methods and faster computing sometimes time constraints, cost, staff, and equipment availability mean that not all incidents are mapped completely, with some portions of incidents being prioritized over others. With this in mind, Houck et al. (2018) classify reconstructions into four main categories; item level, single incident level, event level, and large scale.

- *Item Level*, where the reconstruction is of a single object of interest such as a firearm.
- *Single incident level*, where the focus is on a portion of a scene such as a broken window or confined space.
- *Event level*, this includes all parts involved in an act such as an entire homicide scene.
- *Large-scale*, these include physically large incidents more commonly associated to natural disasters, accidents and acts of terrorism.

With considerations to these classifications, multi-method approaches are often used to ensure an acceptable level of accuracy is achieved. Therefore, this next section explores past and present reconstruction techniques, exploring limitations and abilities of each approach, then this entry concludes with the outlining of state-of-the-art techniques.

Reconstruction Techniques

Sketches and Drawing

The role of scene reconstruction in investigations was acknowledged early on in Hans Gross's

(1893) Handbook for Examining Magistrates as a System of Criminology (later translated by Adam and Adam 1962). Although a great deal of time has passed since this publication, scene sketches are still the most common practice for crime scene reconstruction (Gardner 2012). The purpose of a scene sketch is to compliment photographs and notes taken at the scene, as typically photographs are later back located onto sketches (Ruffell et al. 2014). Generally, initial scene sketches are not to scale, however, scale and measurements should be recorded where possible and added to sketches using established recording methods (Houck et al. 2018). Although this method is tried and tested in crime scene reconstructions (Gardner 2012), upscaling this approach to large accident and disaster scenes is challenging due to the scale and complexity of these incidents and the time-consuming nature of the method.

However, in small-scale scenarios where a sketch may be more appropriate, the sketch can be refined and redrawn using Computer Aided Design (CAD) software after the fact providing associated measurements have been recorded (Houck et al. 2018). These Three-dimensional (3D) CAD drawings are a commonplace technique as the investigator can introduce and move scaled objects within the drawing such as people, weapons, or furniture to better recreate the environment. Although these reconstructions provide clear context of evidence to investigators and jurors to corroborate or disprove testimonies, the nature of these sketches makes them subjective and limited in application.

Laser Scanning

Better suited for large-scale scene reconstructions, terrestrial laser scanners are increasingly used due to their increased range (350 m) compared to other optical techniques (Carew and Errickson 2019; FARO 2019). These scanners operate based upon either continuous frequency modulated (phase-shift) or pulsed (time of flight) techniques to determine distances to objects (Zhang 2013). Many of these systems have internally or externally moving parts to allow data to be captured in 360°, this enables the recording of hundreds of thousands of points per second. However, to cover large environments and reconstruct scenes without shadows the scanner must be moved to capture unseen surfaces. Depending upon the type of system the merging of scans may be done automatically in associated software with or without the aid of markers (FARO 2019). Some device software may also allow for the point cloud information to be exported into CAD software to introduce and manipulate objects as outlined above. However, although these devices are capable of capturing true color environments with fast acquisition and processing time (Buck et al. 2013), these systems can cost in excess of $40,000 limiting their popularity (Carew and Errickson 2019).

Structured Light

In contrast to large-scale laser scanning, structured light is better suited to smaller-scale target objects and surfaces, such as the impact region of a car involved in a road traffic accident. Structured light is the process of projecting a pattern of light onto a target surface and recording the visual deformities caused by that target surface using a camera (Zhang 2013). Due to the nature of structured light, it is best suited for small object/item level modelling, for example, firearms or weapons, as opposed to complete scene recording. However, structured light is capable of recording geometric, morphometric, and color-surface data (Sansoni et al. 2009), and also has fast acquisition and processing times although this is dependent on computational power (McPherron et al. 2009).

Photogrammetry

Having gained significant popularity over recent years, photogrammetry is the practice of obtaining distances and geometric properties from two dimensional (2D) images using single or multiple camera approaches (Hartley and Zisserman 2003). The most common of these approaches used today is Structure from Motion (SfM). SfM is a photo-realistic reconstruction technique that relies upon features being detected and matched across a sequence of images to register camera locations and 3D structure (Lowe 2004; Smith et al. 2016). Recent advancements in digital cameras and

computer vision techniques has made SfM an affordable practical investigation tool without the requirement of specialist professionals (Edelman and Aalders 2018). Additionally, comparative studies by Baier and Rando (2016) have shown that SfM is comparable in accuracy to laser scanning techniques with much shorter recording time and less expense. This is a critical consideration when pressure is there to release a scene. However, extended processing time compared to other techniques was noted in multiple cases (Marcin et al. 2017; Urbanová et al. 2017). In addition to this, the resultant 3D model quality is affected by camera quality and basic knowledge of the user (Edelman and Aalders 2018) as well as the presence of texture within the target environment (Marcin et al. 2017).

State of the Art

Using a range of techniques outlined above as well as others, current state-of-the-art reconstruction methods include the use of Unmanned Aerial Vehicles (UAVs) (see entry ▶ "Drones") equipped with airborne laser scanning systems or cameras for the purpose of SfM. Similar to the methods outlined above, UAVs often use specific designed devices to capture aerial data. Experiments of UAV-based scene recording include on-site body documentation (Urbanová et al. 2017) and road traffic accidents (Pix4D 2019). Having already proven popular in large-scale and outdoor environments both as a tool for orthomosaics and 3D modelling, it is likely that this technology will move indoors. Although the forensic effectiveness of UAV technology within indoor environments is still being established (Bucknell and Bassindale 2017; Parrott et al. 2018).

Despite some of the limitations outlined within these sections, all digital techniques allow for the indefinite digital preservation of an incident scene which allows investigators to revisit the scene at any point once the scene has been released (Edelman and Aalders 2018). With regard to visualizing these results, Koller et al. (2019) propose the use of Virtual Reality (VR) as a useful visualization tool for both training/teaching as well as in the courtroom. 3D modelling is also impacting the courtroom by enabling items to be 3D printed and physically presented to jurors at court (Baier et al. 2018).

Conclusion

To summarize, over recent years our ability to record and reconstruct environments for investigative purposes has advanced dramatically through technological developments, from physical clay modelling and hand-drawn sketches to complete 3D digital reconstructions captured using UAVs and visualized through VR. Largely, reconstruction is beneficial for the investigator to be able to view a scenario in a cohesive manner with all the information available at once, as opposed to flicking through photographs, witness statements, and measurements simultaneously. This overall perspective allows investigators to challenge testimonies and determine the sequence of events more efficiently. A trend that is clear to see from these reconstruction techniques is that as the usability and accuracy of the technology improves, so does the cost, which in most cases is often an overwhelming factor to inhibit progression. Although the value of some of this technology is yet to be fully realized amongst practitioners, as future work emerges on the capabilities and limitations of this technology within a forensic forum, it is likely that many of the technologies outlined earlier will become increasingly common place.

Cross-References

▶ Drones

References

AAIB. (2017). Annual safety review 2016. AAIB – Air Accidents Investigation Branch. Retrieved from www.aaib.gov.uk

ACSR. (2019). ACSR – Association for Crime Scene Reconstruction. Retrieved Feburary 26, 2019, from https://www.acsr.org/

Adam, J., & Adam, J. (1962). *Criminal investigation. Adapted from the System der Kriminalistik of Dr. Hans Gross*. London: Sweet & Maxwell.

Baier, W., & Rando, C. (2016). Developing the use of structure-from-motion in mass grave documentation. *Forensic Science International, 261*, 19–25. https://doi.org/10.1016/J.FORSCIINT.2015.12.008.

Baier, W., Warnett, J. M., Payne, M., & Williams, M. A. (2018). Introducing 3D printed models as demonstrative evidence at criminal trials. *Journal of Forensic Sciences, 63*(4), 1298–1302. https://doi.org/10.1111/1556-4029.13700.

Buck, U., Naether, S., Braun, M., Bolliger, S., Friederich, H., Jackowski, C., . . . Thali, M. J. (2007). Application of 3D documentation and geometric reconstruction methods in traffic accident analysis: With high resolution surface scanning, radiological MSCT/MRI scanning and real data based animation. *Forensic Science International*, *170*(1), 20–28. https://doi.org/10.1016/j.forsciint.2006.08.024.

Buck, U., Naether, S., Räss, B., & Thali, M. J. (2013). Accident or homicide – Virtual crime scene reconstruction using 3D methods. *Forensic Science International, 225*(1–3), 75–84. https://doi.org/10.1016/J.FORSCIINT.2012.05.015.

Bucknell, A., & Bassindale, T. (2017). An investigation into the effect of surveillance drones on textile evidence at crime scenes. *Science & Justice, 57*(5), 373–375. https://doi.org/10.1016/J.SCIJUS.2017.05.004.

Carew, R. M., & Errickson, D. (2019). Imaging in forensic science: Five years on. *Journal of Forensic Radiology and Imaging, 16*, 24–33. https://doi.org/10.1016/J.JOFRI.2019.01.002.

Chisum, W. J., & Turvey, B. E. (2011). *Crime reconstruction* (2nd ed.). London: Academic/Elsevier.

Edelman, G. J., & Aalders, M. C. (2018). Photogrammetry using visible, infrared, hyperspectral and thermal imaging of crime scenes. *Forensic Science International, 292*, 181–189. https://doi.org/10.1016/J.FORSCIINT.2018.09.025.

FARO. (2019). FARO focus 3D laser scanner – FARO Technologies UK Ltd. Retrieved February 28, 2019, from https://www.faro.com/en-gb/products/construction-bim-cim/faro-focus/

Gardner, R. M. (2012). *Practical crime scene processing and investigation* (2nd ed.). New York: CRC Press.

Gross, H. (1893). Handbook for Examining Magistrates as a System of Criminology.

Hartley, R., & Zisserman, A. (2003). *Multiple view geometry in computer vision*. Cambridge, UK: Cambridge University Press.

Houck, M. M., Crispino, F., McAdam, T., Houck, M. M., Crispino, F., & McAdam, T. (2018). Crime scene reconstruction. In *The science of crime scenes* (pp. 341–344). London: Academic. https://doi.org/10.1016/B978-0-12-849878-1.00024-7.

Koller, S., Ebert, L. C., Martinez, R. M., & Sieberth, T. (2019). Using virtual reality for forensic examinations of injuries. *Forensic Science International, 295*. https://doi.org/10.1016/j.forsciint.2018.11.006.

Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision, 60*(2), 91–110. https://doi.org/10.1023/B:VISI.0000029664.99615.94.

Marcin, A., Maciej, S., Robert, S., & Wozniak, A. (2017). Hierarchical, three-dimensional measurement system for crime scene scanning. *Journal of Forensic Sciences, 62*(4), 889–899. https://doi.org/10.1111/1556-4029.13382.

McPherron, S. P., Gernat, T., & Hublin, J.-J. (2009). Structured light scanning for high-resolution documentation of in situ archaeological finds. *Journal of Archaeological Science, 36*(1), 19–24. https://doi.org/10.1016/J.JAS.2008.06.028.

Parrott, E., Pointon, H., Bezombes, F., & Panter, H. (2018). Understanding evidence dispersal caused by the effects of using unmanned aerial vehicles in active indoor crime scenes. *World Academy of Science, Engineering and Technology, 12*(6), 1. Retrieved from https://waset.org/pdf/books/?id=84770&pageNumber=1.

Pix4D. (2019). Retrieved February 28, 2019, from https://www.pix4d.com/industry/public-safety

Ruffell, A., Pringle, J. K., & Forbes, S. (2014). Search protocols for hidden forensic objects beneath floors and within walls. *Forensic Science International, 237*, 137–145. https://doi.org/10.1016/J.FORSCIINT.2013.12.036.

Sansoni, G., Trebeschi, M., & Docchio, F. (2009). State-of-the-art and applications of 3D imaging sensors in industry, cultural heritage, medicine, and criminal investigation. *Sensors, 9*(1), 568–601. https://doi.org/10.3390/s90100568.

Smith, M. W., Carrivick, J. L., & Quincey, D. J. (2016). Structure from motion photogrammetry in physical geography. *Progress in Physical Geography: Earth and Environment, 40*(2), 247–275. https://doi.org/10.1177/0309133315615805.

Urbanová, P., Jurda, M., Vojtíšek, T., & Krajsa, J. (2017). Using drone-mounted cameras for on-site body documentation: 3D mapping and active survey. *Forensic Science International, 281*, 52–62. https://doi.org/10.1016/j.forsciint.2017.10.027.

Zhang, S. (2013). *Handbook of 3D machine vision: Optical metrology and imaging*. New York: CRC Press/Taylor & Francis Group.

Further Reading

Carew, R. M., & Errickson, D. (2019). Imaging in forensic science: Five years on. *Journal of Forensic Radiology and Imaging, 16*, 24–33. https://doi.org/10.1016/J.JOFRI.2019.01.002.

Chisum, W. J., & Turvey, B. E. (2011). *Crime reconstruction* (2nd ed.). London: Academic/Elsevier.

Houck, M. M., Crispino, F., McAdam, T., Houck, M. M., Crispino, F., & McAdam, T. (2018). Crime scene reconstruction. In *The science of crime scenes* (pp. 341–344). London: Academic. https://doi.org/10.1016/B978-0-12-849878-1.00024-7.

Smith, M. W., Carrivick, J. L., & Quincey, D. J. (2016). Structure from motion photogrammetry in physical geography. *Progress in Physical Geography: Earth and Environment, 40*(2), 247–275. https://doi.org/10.1177/0309133315615805.

Investigations: Bank Fraud

Sonny Smith
Texas A&M University, College Station, TX, USA

Keywords
Check kiting · Credit card fraud · Forgery · Shoulder surging · Skimming · Social engineering · White collar crime

Definition

Fraud, as an all-encompassing term, is a problem that has negatively affected institutions across the world to the tune of approximately $3.5 trillion per year, with $16.8 billion in US losses (Pascual et al. 2018). In 2014, McAfee and the Center for Strategic and International Studies found the losses from cybercrime alone to be between $375 and $575 billion per year (Insurance Information Institute 2018). Schemes such as identity fraud, credit card fraud, skimming, wire fraud, check tampering, and financial statement fraud have been some of the more common and lucrative methods employed in these schemes. These fraud schemes impact multiple sectors of society, such as government and public service organizations, individuals, financial institutions, online retailers, and traditional brick and mortar merchants.

> *"Data! Data! Data!" he cried impatiently. "I can't make bricks without clay."*
> Sherlock Holmes
> –The Adventure of the Abbey Grange

Introduction

Just as Sherlock Holmes implored Watson, clay, or data (information/clues) in this case, is the key ingredient to making bricks (solving crimes). The more information and clues an investigator can obtain, the stronger the case will be, and the better the chances of catching the perpetrator/s. Depending on the investigation, obtaining the needed data can be as simple as reviewing video footage, collecting fingerprints, or even convincing a suspect to incriminate himself or his group through a thorough interrogation; however, with the advance of technology, obtaining data has become ever more difficult, as criminals have found unique and intricate ways to perpetrate their schemes and hide their steps. These intricate and unique methods of evasion have become more evident in the growing complexity of bank fraud schemes.

Despite these complexities, the general principles of the investigative process remain the same. In essence, the investigator is looking to answer the who, what, when, where, why, and how of the issue at hand. Many times, a number of the variables may already be known, and the investigator must then set out to compile the additional data needed to put the pieces together and complete the rest of the investigative puzzle. In other instances, there are no known facts other than the knowledge that an incident has occurred; thus, the investigator must start with a blank slate in the hopes of determining what has happened and who or what is responsible for it.

The purpose of this entry is to provide an overview of bank fraud and the investigative process. The general topic of bank fraud and investigating bank fraud as an offense is a very complex topic, with many interconnecting criminal elements and schemes, as well as investigative relationships between the public and private sector. Because of these factors and the limited space available for this topic, this entry will provide an overview of these complexities and relationships. The entry will be divided into four (4) sections, with Section I "Introduction and Terms" introducing fraud in general and bank fraud in particular, as well as providing a list of useful definitions. Section II will focus on the "Who" component and will be divided into two subsections: (1) who are the individual(s) committing the crimes and (2) who are groups investigating the crimes. Section III will explore the "What" component; what are some of the more prevalent schemes or crimes being perpetrated? This section will be used to provide examples of the most

prominent bank fraud schemes. Section IV will explore "How" investigators are working together to combat these schemes. The three missing components, *when*, *where*, and *why*, will not be addressed here individually, as they will be addressed indirectly throughout the other sections.

Introduction and Terms

Fraud, as an all-encompassing term, is a problem that has negatively affected institutions across the world to the tune of approximately $3.5 trillion per year, with $16.8 billion in US losses (Pascual et al. 2018). In 2014, McAfee and the Center for Strategic and International Studies found the losses from cybercrime alone to be between $375 and $575 billion per year (Insurance Information Institute 2018). Schemes such as identity fraud, credit card fraud, skimming, wire fraud, check tampering, and financial statement fraud have been some of the more common and lucrative methods employed in these schemes. These fraud schemes impact multiple sectors of society, such as government and public service organizations, individuals, financial institutions, online retailers, and traditional brick and mortar merchants.

While the total dollar amount of fraud may be a daunting figure, it only accounts for the total amount that has been reported. Some individuals and organizations do not report losses for several reasons (underreporting to shareholders, embarrassment, and not knowing fraud is being committed); therefore, the actual figures may be much higher than the reports shown. Irrespective of those who fail to report, what the trending data reveals of those known losses is that the number of fraud schemes and losses is growing, becoming more complex, and they are responsible for approximately 5% of organization losses annually (Association of Certified Fraud Examiners 2018). Bank fraud, in particular, has become an ever-growing problem for federal and state law enforcement and private sector investigators to combat due to the complexity of the types of schemes being perpetrated. The schemes in question are a by-product of a growing problem of identity theft and cybercrime. These complex relationships, in turn, have required financial industries, in conjunction with federal, state, local, and private investigative sectors to continually employ methods to keep up with those schemes.

For example, according to a 2018 fraud report from Javelin Strategy & Research, the increases and complexities of the schemes from 2016 to 2017 in the USA have revealed a 120% increase in the number of card-not-present fraud schemes, which is when transactions are made online or via a phone where the physical card is not required to complete the purchase. The rise of card-not-present schemes appeared to coincide with the new regulations requiring EMV technology to be used on credit and debit cards, thus making it more difficult for criminals to make in-store purchases with counterfeit credit or debit cards. Criminals, in response to the rise of EMV technology, have resorted to making online purchases. In this example, investigators must work with merchants and financial institutions to find ways to address this type of fraud.

While the schemes have increased in complexity, the victims of those schemes have remained constant, as have the federal and state criminal codes. At the federal level, the bank fraud criminal code addresses any act or throughway (Internet, wire fraud; snail mail, mail fraud) in which one either attempts or successfully completes the criminal act. It can be a single charge comprising several offenses such as forging or using counterfeit financial documents, embezzlement, falsifying information on financial applications, check kiting, forgery and altered checks, using or producing counterfeit or altered access devices, and mail fraud. Bank fraud can also be charged in conjunction with any of the previous noted offenses. For instance, you can have a single bank fraud charge and a single charge of credit card fraud and wire fraud. It is oftentimes an element of a cyber theft in which a computer is used to further crimes such as embezzlement, fraud, and theft of financial data.

While there are many offenses that can constitute a single bank fraud charge at the

federal level, bank fraud, at the state level does not, in most cases, have a single bank fraud criminal offense. Rather, most states have dozens of statutes addressing the various offenses. Therefore, there is no single "bank fraud" state charge that was found; instead, there are a variety of infractions that on its own constitute a crime against a financial institution. For instance, in New York State, a wide range of fraud offenses, such as issuing a bad check, forgery, fraud in solvency, and fraud involving a security interest, can fit within the "bank fraud" category (Article 190-New York State Penal Code 2018). Likewise, in California and Texas, there are also a variety of offenses that fall into the bank fraud category. In California, there are check fraud; credit card, debit card, and access card fraud; and forgery and bad check charges that fall under the "bank fraud" category (Penal Code 470 PC, California's Forgery Law 2018). Likewise, in Texas, there are also many forgery laws that fall under the bank fraud category such as forgery, credit card or debit card abuse, false statement to obtain property or credit or in the provision of certain services, credit card transaction record laundering, and misapplication of fiduciary property or property of financial institution (Texas Penal Code – Chapter 32-Fraud 2018). Although each state may have different codes and processes used to prosecute these offenses, the common denominator between them is their use in prosecuting fraud committed against financial institutions.

Terms

Access device – means any card, plate, code, and account number that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value or that can be used to initiate a transfer of funds (other than a transfer originated solely by a paper instrument).

Bank fraud – the criminal act that occurs when a person or persons uses illegal means to receive or attempt to receive money or assets from a bank or other financial institution. This definition includes fraud by falsely posing as a financial institution.

Check kiting – a type of check fraud in which an individual takes advantage of "the float" to make use of nonexistent funds in a checking or bank account. The float is duplicate money found in a bank account during the time between a deposit being made into the recipient's account and debited from the sender's account.

Counterfeit access device – means any access device that is counterfeit, fictitious, altered, or forged or an identifiable component of an access device or a counterfeit access device.

Credit card fraud – any theft or fraud committed or attempted involving a payment card.

Dumpster diving – the act of digging through a trashcan or dumpster to obtain personal or business documents that contain PII or financial data.

EMV technology – named after the companies that first developed and implemented the technology (Europay, MasterCard, and Visa), this type of technology has a microchip embedded in the card that stores and protects the cardholders' data. The EMV replaces the need for the magnetic strip on the back of the credit/debit card, which is less secure.

Federal Deposit Insurance Corporation (FDIC) – is an independent agency created by Congress in 1933, as part of the 1933 Banking Act during the Great Depression to restore trust in the US banking industry. The FDIC initially insured up to $2500, but now it insures up to $250,000 in assets.

Financial institution – is defined by federal law to include banks and credit unions that are federally insured, such as by the Federal Deposit Insurance Corporation (FDIC), Federal Reserve banks, mortgage lending businesses, and certain other institutions that accept deposits of money and other assets.

Forgery – is the making of a fake document, the modification of an existing document, or the unauthorized signing of a signature without prior authorization.

Fraud – deception intended to result in financial or personal gain.

Identity fraud – the use of one person's identification by another without prior authorization involving fraud or deception.

Mail fraud – any fraudulent scheme perpetrated via mail services.

Mail theft – when an individual(s) removes mail that may contain PII, credit card information, or bank statements.

Personally identifiable information (PII) – any personal information that could be used to identify a specific person and distinguish one person from another. Common PII data can be found in one's Social Security Card, birth certificate, personal check, or driver's license.

Scheme – make plans, especially in a devious way or with intent to do something illegal or wrong.

Securities Investor Protection Corporation (SIPC) – was mandated by Congress in 1970, as part of the Securities Investor Protection Act (SPIA). SIPC covers up to the first $500,000 invested in stocks or money market accounts.

Shoulder surfing – the act of spying on someone using an ATM or other devices in an attempt to obtain PII or access and personal financial data.

Skimming – this can occur at restaurants, ATM's, gas stations, or other types of venues that are heavily trafficked. Criminal instruments known as skimming devices can be as small as a handheld swiped device, or it can be affixed to the front of an ATM or a gas pump where customers insert their credit or debit cards. The skimming devices, which are readily available online, capture the relevant information embedded within the credit or debit cards (credit card number, name, and CVC number) which is then either downloaded via USB or wirelessly transferred where it can then be embedded onto a "white card," a counterfeit credit or debit card, or stored to make illicit online transactions. In most instances, the victim doesn't know their information has been stolen until they start receiving statements showing the illicit transactions or if they see their bank accounts have been compromised.

Social engineering – when an individual, in person, over the telephone, or by computer, deceives an individual into divulging their PII and other sensitive information.

White collar crime – financially motivated, nonviolent crime usually associated business and government professionals.

Wire fraud – any fraudulent scheme perpetrated via Internet or wired services.

Who

Who: Part I – The Criminal Element

The types of individuals who commit bank fraud are as diverse as the schemes themselves. They range from the individual lone actor who might be a bank employee or a waiter at the local restaurant to a cyber-criminal organization that operates online and has a vast amount of technical expertise at hacking into databases and evading law enforcement technical experts. The criminal element has remained an essentially faceless group who have used their technological skills to collaborate in schemes from across the globe, while using cyberspace to remain anonymous.

Despite their ability to remain anonymous, law enforcement groups have made inroads into the various types of criminal groups and their general regional bases of operations. According to a report titled *The New Mafia: Gangs and Vigilantes*-A Guide to Cybercrime for CEOs (Malwarebytes 2017), cybercriminals can be divided into four groups: traditional gangs, state-sponsored attackers, ideological hackers, and hackers for hire. Two of the more relevant gang types to this entry are the traditional and state-sponsored gangs. Traditional gangs have the same goal in mind as their drug and crime gang counterparts, to obtain as much money as possible, as quickly as possible. In many instances, these traditional cybercrime gangs are the same individuals connected to traditional drug and crime organizations, who band together as experienced hackers and attempt to use their expertise to attack and disrupt individuals and organizations via the Internet. State-sponsored gangs have received a lot of recognition lately, with the investigations into Russian government sponsored interference in the 2016 US Presidential election. Before then, state-sponsored hackers from Russia, North Korea, and China were primarily thought to be the primary actors perpetrating data breaches and phishing schemes. Although they are often times credited

with international espionage incidences, they are beginning to participate in corporate theft and sabotage (Malwarebytes 2017).

In regard to bank fraud schemes in particular, a look at the FBI's Top 5 Most Wanted for Cybercrimes reveals four Russian (4) and a group of seven (7) Iranians wanted for a variety of bank fraud and data breach schemes (Park 2017). Similar to the FBI's Cybercrimes list, law enforcements groups have placed the larger cybercriminal operations in Russia, China, and North Korea. Individually, however, anyone in any location can their computer to capture PII and financial data.

Who: Part II – Law Enforcement

There is some confusion about which law enforcement agency is the primary agency responsible for investigating bank fraud offenses. The reason for this confusion is twofold: The first is because both the US Secret Service and the Federal Bureau of Investigations (FBI) investigate bank fraud, sometimes individually, sometimes jointly, and sometimes as members of Financial Fraud Task Forces. The second reason for the confusion stems from the types of bank fraud for which each is responsible.

The Secret Service, initially created in 1865, as an investigative division within the Department of Treasury took on the tasks of investigating rampant counterfeiting following the Civil War, Klan activity, and bank robbery. While it is primarily known as the agency that provides protection for the president and vice president, it wasn't until the assignation of President William McKinley in 1901 that it began carrying out those tasks. Secret Service duties expanded even further with the passage of the Comprehensive Crime Control Act of 1984, which expanded its jurisdiction to include identity fraud (18 US Code 1028), credit card fraud (18 US Code 1029), and computer fraud (18 USC 1030). The Secret Service has also established a Financial Crimes Task Force (FCTF) comprised of state, local, and federal law enforcement agencies, as well as private entities, to encourage interagency and private sector collaboration on financial crimes investigations, as well as a Cybercrime Task Force (ECTF) to investigate cybercrime.

While its initial mission did not start out as diverse as that of the US Secret Service, the FBI was created in 1908 by US Attorney General Charles J. Bonaparte, as a "regular force of special agents available to investigate certain cases of the Department of Justice (White-Collar Crime 2016)." The difference in the types of bank fraud cases they work, which differs from the Secret Service, is that the FBI targets "sophisticated, multi-layered fraud cases that harm the economy (White-Collar Crime 2016)." Therefore, its major focus is on crimes such as corporate fraud, securities and exchange fraud, mortgage fraud, and money laundering. The FBI also has its own Financial Fraud Enforcement Task Force that works with its federal partners and local agencies to investigate large-scale criminal enterprises (White-Collar Crime 2016).

To accomplish their missions, the FBI and Secret Service both work closely with the Securities and Exchange Commission, the Internal Revenue Service, the US Postal Inspection Service, the Commodity Futures Trading Commission, and the Treasury Department's Financial Crimes Enforcement Network, as well as state and local law enforcement agencies (White-Collar Crime 2016).

> *The case is one where we have been compelled to reason backward from effects to causes.*
> Sherlock Holmes
> The Adventure of the Cardboard Box

What

Schemes: What Are the Criminals Doing?

As outlined in the Introduction, there are times when investigators are unaware of specifics other than the fact that some suspicious activity has occurred or is occurring. Similar to the Sherlock Holmes quote above this heading, investigators must work the case backward in an effort to determine what has happened and how it has happened. What is known in general is that the criminal element is trying to find as much PII and financial date as possible so they can convert that data into cash or goods. How they accomplish this is by looking for and developing avenues upon which to prey on technical and nontechnical vulnerabilities.

Technical vulnerabilities can come in the form of computer and Internet avenues, (data breaches, phishing, malware social engineering schemes), otherwise, known as cybercrime. According to the US Secret Service, "evidence in criminal investigations is often scattered across numerous domestic and international jurisdictions, and may be held by a wide range of technology providers and digital devices (The Investigative Mission 2018)." The digital devices previously noted come in the form of small handheld scanners or computer devices used in skimming and jackpotting schemes. Nontechnical vulnerabilities can be described as acts such as shoulder surfing, mail theft, and dumpster diving.

Some of the methods used by criminals to collect PII and financial data rely on a combination of both technical and nontechnical vulnerabilities. An insider threat is a vulnerability that can straddle both the technical and nontechnical variables, as you can have a person working for a merchant or financial institution, for example, who uses their position to obtain the PII or financial data of customers and then use that information to commit various bank fraud crimes themselves or as part of a criminal enterprise. Irrespective of how the data is collected, criminals are quickly able to put that data to work, to illicit as much cash, in as quickly a time frame as possible.

The following list of schemes are some examples of the types of methods used by the criminal element to gather and then use PII and financial data. In many of these examples, the schemes identified are the second offenses committed, with the first being identity theft. For instance, an individual can be a victim of identity theft, which will then lead to criminals obtaining credit cards in the victim's name, submitting fraudulent loan applications, or opening new checking accounts or compromising existing accounts (Pascual et al. 2018).

Schemes

Data breaching – a form of cyber theft wherein sensitive data is stolen via computer hacking. There have been several high-level breaches since 2005. One of the more well-known and most recent instances was the 2017 Equifax breach where 143 million customer accounts and credit card data were compromised. In 2014, Yahoo had upwards of three billion accounts compromised. In 2013, target stores had 100 million accounts compromised costing them approximately $162 million, and Heartland Payment Systems had 134 million accounts compromised in 2008 costing the company $145 million to cover fraudulent payments. In January 2016, Austrian-based aerospace company FACC suffered an approximate €42 million ($47 million) theft via a hacking incident (Reuters 2016).

Data breaches were not solely confined to private entities however. In 2015, the Office of Personnel Management (OPM) revealed the PII of 21.5 million current and former federal employees with security clearances had been compromised. Also in 2015, the US Voter Database was incorrectly configured resulting in the release of the PII for over 191 million voters in all 50 states and the District of Columbia (Finkle and Volz 2015). In 2016, the Federal Bureau of Investigations was hacked, resulting in the release of the PII of over 20,000 employees.

Card-not-present fraud – this scheme is one of the elements resulting from skimming in which criminals will use the stolen credit card information to make online, rather than in person purchases. This type of fraud is expected to rise as more industries convert their credit card readers to accept the EMV chip technology used by merchants (ACFE 2018).

Account take-over fraud – criminals will use stolen information to access victim's financial account in an effort to withdraw or transfer funds. According to the JAVELIN Report (2018), this scheme increased 120% from 2016 to 2017 and resulted in $5.1 billion in fraud losses.

Jackpotting – this scheme is relatively new in the USA but has been previously committed in Europe and Mexico (Langone 2018). Jackpotting occurs when an individual/s poses as an ATM technician and uses an ATM key (which are readily available online) to gain access to the

inside of the ATM. A programmed laptop and cellphone are installed inside the ATM so the machine can be taken over remotely and forced to discharge cash at a rate of up to 40 bills every 23 s. According to the US Secret Service, the ATM will spit out money like a slot machine in a casino after someone hits the jackpot (Langone 2018). This scheme relies on multiple people as one person will act as the ATM technician, while others act as ATM customers to withdraw the illicit funds.

Forged or altered checks – an individual/s will steal or manufacture checks (by any of the methods previously outlined) to assume control of the funds in a legitimate bank account or to withdraw funds from counterfeit checking accounts. Criminals can alter legitimate checks and change the name of the intended payee, and in the case of stolen checks, thieves may forge the account holders' signature and write checks to an accomplice with a counterfeit identification, who will cash the stolen check.

Phishing – a social engineering crime in which an individual(s) is contacted by email, telephone, or some other method by someone who poses as a legitimate business or organization and attempts to coerce that individual to reveal sensitive PII or passwords, bank, and/or credit/debit card data. Phishers oftentimes create webpages similar in appearance to those of legitimate banks or other financial institutions and ask the respondent for PII to "verify" account information. Once the PII is entered, the Phishers can use the respondent's data to commit any number of fraudulent offenses.

Insider threat – this type of scheme involves an employee working at a merchant or financial institution who collects relevant data of customers and then either sells the information or uses that information to carry out fraudulent criminal activity.

Malware attack – a victim has an unprotected or not fully protected computer and is hit with a malware. This malware provides the criminal the ability to compromise that person's email account and monitor all email activity. The victim types passwords for a financial institution account, which gives the criminal an opportunity to access the account and transfer funds or open other fraudulent accounts in the victim's name.

What one man can invent another can discover.
Sherlock Holmes
–The Adventure of the Dancing Man

How

How Are State, Local, Federal, and Private Investigators Approaching Cases?

The Investigative Process

According to Bennett and Hess (2004), an investigation is a simple fact finding and reporting process that follows a patient, step-by-step process (4). Osterburg (1981) noted the process to be akin to the scientific method of solving problems, and it follows the five primary steps of the scientific method: stating the problem, forming the hypothesis, collecting the data by observing and experimenting, interpreting these data, and drawing conclusions. In the first step of the process, identifying the problem, the investigator must determine if a crime has been committed or if there is another explanation that would account for the current situation? In the second step, the hypothesis stage, questions can be raised about suspicious activities; "there appears to be a pattern of bank fraud committed with counterfeit credit cards." Step 3, the data collection phase, can be achieved through a combination of processes such as observation (stakeouts, reviewing video, etc.) and review of records or data files and/or through witness and victim interviews. Once the data has been collected, the next step is to analyze all the information. This step consists of sending evidence to the lab for analysis, conducting a more detailed review of the interviews, and possibly conducting more in-depth interviews. The final stage of the process is when the investigator has drawn a conclusion. This occurs when the investigator has determined who has committed the crime, with certainty.

While the investigative processes are similar between the two groups, the term "with certainty" is an important term to consider when

differentiating between public law enforcement investigators and private sector investigators. It can also be described as "burden of proof" or "fact beyond a reasonable doubt." Whichever term one wants to use, the way evidence is used is much more stringent for public sector law enforcement agencies, than it is for private sector investigators. Sennewald and Tsukayama (2015) explored this concept and others, as they related to the investigative practices employed by law enforcement and private sector investigators. They noted they are primarily the same with a few notable exceptions: the first being the objectives of both groups. Private sector investigators serve the interests of the organization of which they are employed, while law enforcement officers are beholden to the public at large. As such, the primary goal of law enforcement is not only to stop the continuation of the criminal activity and recouping the losses, but to also apprehend and punish the criminal's responsible for the criminal activity. A private sector investigator, however, may not have those same interests in mind, as the primary goal is to stop the activity and recoup the losses. They may not have any interest in public punishment of the criminal, as it might reflect poorly upon the organization because the investigation may expose lax financial or data controls employed by the organization. The second notable difference lies with the legal authority of each group. State, local, and federal law enforcements have their authority to conduct investigations and make arrests embedded in constitutional and state laws. Private sector investigators, on the other hand, are not constitutionally bound by Fourth Amendment rules, nor are they bound by Miranda rules.

Some private sector investigators will work cases independent of law enforcement, while the creation of task forces, like the US Secret Service Electronic Crimes Task Forces (ECTF) and Financial Crimes Task Forces (FCTF), has provided a working network of law enforcement and private sector investigators to work together in an information sharing capacity to address the growing threats of fraud to the financial industries. When working collectively in task force environments or when a law enforcement and a private sector investigator work together to investigate a singular crime, the relationship is geared toward the law enforcement goals previously outlined. The relationship also allows the groups to enhance their investigative performances by sharing their complimentary skills, experiences, knowledge, and resources.

Conclusion

While the success of bank fraud schemes has increased over the years with the growth of technology and the Internet, law enforcement and private sector investigators must remain vigilant in their efforts to collaborate in task forces and with information sharing. Achieving any level of success against the criminal element will require greater technological strides and outreach efforts to the public about the technological and non-technological vulnerabilities open to exploitation.

Cross-References

- ▶ Criminals: Cybercriminals
- ▶ Criminals: White-Collar Crimes
- ▶ Cybersecurity: Practice
- ▶ Investigations: Criminal
- ▶ Investigations: Cybercrimes
- ▶ Investigations: Fraud

References

2016 New York Laws :: PEN – Penal :: Part 3 – SPECIFIC OFFENSES :: Title K – OFFENSES INVOLVING FRAUD :: Article 190 – (190.00 – 190.89) OTHER FRAUDS :: 190.05 – Issuing a bad check. (n.d.). Retrieved 1 May 2018, from https://law.justia.com/codes/new-york/2016/pen/part-3/title-k/article-190/190.05

ACFE Report to the Nations | 2018 Global Fraud Study. (2018). Retrieved 13 Apr 2018, from http://www.acfe.com/report-to-the-nations/2018/

Austria's FACC, hit by cyber fraud, fires CEO. (2016, May 25). Retrieved 20 Apr 2018, from https://www.reuters.com/article/us-facc-ceo/austrias-facc-hit-by-cyber-fraud-fires-ceo-idUSKCN0YG0ZF.

Bennett, W. W., & Hess, K. M. (2004). *Criminal investigation* (7th ed.). Belmont: Wadsworth/Thompson.

California Code, Penal Code – PEN § 470. (n.d.). Retrieved 1 May 2018, from https://codes.findlaw.com/ca/penal-code/pen-sect-470.html.
Facts + Statistics: Identity theft and cybercrime. (n.d.). Retrieved 15 Apr 2018, from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.
Finkle, J., & Volz, D. (2015, December 29). Database of 191 million U.S. voters exposed on Internet: Researcher. Retrieved 1 Apr 2018, from https://www.reuters.com/article/us-usa-voters-breach/database-of-191-million-u-s-voters-exposed-on-internet-researcher-idUSKBN0UB1E020151229.
Langone, A. (2018, January 30). What is ATM jackpotting? and how to protect yourself | money. Retrieved 27 Mar 2018, from http://www.time.com/money/5125106/what-is-atm-jackpotting/
Malwarebytes (Ed.). (2017). The new mafia: Gangs and vigilantes-A guide to cybercrime for CEO's. Retrieved 1 Apr 2018, from https://www.malwarebytes.com/pdf/white-papers/Cybercrime_NewMafia.pdf.
Osterburg, J. W. (1981). Scientific method and criminal investigation. *Journal of Police Science and Administration, 9*(2), 135–142. Retrieved 5 Apr 2018.
Park, M. (2017, March 16). Meet the FBI's top 5 most wanted for cyber crimes. Retrieved 27 Apr 2018, from https://www.cnn.com/2017/03/16/us/fbi-most-wanted-cyber-crimes/index.html
Pascual, A., Marchini, K., & Miller, S. (2018, February 06). 2018 identity fraud: Fraud enters a new era of complexity. Retrieved 20 May 2018, from https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
PENAL CODE CHAPTER 37. PERJURY AND OTHER FALSIFICATION. (n.d.). Retrieved 1 May 2018, from https://statutes.capitol.texas.gov/Docs/PE/htm/PE.37.htm
Sennewald, C. A., & Tsukayama, J. K. (2015). *The process of investigation: Concepts and strategies for investigators in the private sector* (4th ed.). Amsterdam: Elsevier Butterworth-Hein.
The Investigative Mission. (2018). Retrieved 1 May 2018, from https://www.secretservice.gov/investigation/.
White-Collar Crime. (2016, May 03). Retrieved 27 Apr 2018, from https://www.fbi.gov/investigate/white-collar-crime

Further Reading

Almandoz, J. (2017). Robert S. Pasley*: Anatomy of a banking scandal: The keystone bank failure – Harbinger of the 2008 financial crisis*.
Biskupic, S. M. (1998). Fine tuning the bank fraud statute: A prosecutor's perspective. *Marq L Rev, 82*, 381.
Dagogo, D. W. (2018). Bank fraud and financial intermediation.
Gottschalk, P. (2018). Characteristics of white-collar crime. In *Investigating white-collar crime* (pp. 1–12). Cham: Springer
Hoffmann, A. O., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking. *The International Journal of Bank Marketing, 30*(5), 390–407.
Hughes, G., Comber, J., & Austin, E. (2018). Insider dealer or unknowing participant: HK court of appeal confirms SFC's broad powers to pursue insider dealing and fraud offences. *Journal of Investment Compliance, 19*, 38–41.
Oa, F. J., & Titiloye, E. O. (2012). Application of continued fractions in controlling bank fraud. *International Journal of Business and Social Science, 3*(9), 210–213.
Smith-Ditizio, A. A., & Smith, A. D. (2018). Computer fraud challenges and its legal implications. In *Encyclopedia of information science and technology* (4th ed., pp. 4837–4848). IGI Global.

Investigations: Burglary

Heather A. Panter
Centre for Advanced Policing Studies, Liverpool John Moores University, Liverpool, UK

Keywords
Residential burglary · Commercial burglary · Burglar modus operandi · Stolen goods conversion

Definition

The FBI's Uniform Crime Reporting (UCR) Program defines burglary as "the unlawful entry of a structure to commit a felony or theft" (FBI 2017). A structure according to UCR includes "an apartment, barn, house trailer, or houseboat when used as a permanent dwelling, office, railroad car (not automobile), stable, or vessel (i.e. ship)" (FBI 2017). Burglary is subdivided into forcible entry, unlawful entry, and attempted forcible entry (FBI 2017). Further, burglary is separated into two distinct categories: (1) residential and (2) commercial. Notably, individual states may have different definitions, classifications, and criminal penalties. Burglary investigations entail appropriate first responder actions, the establishment of a burglar (s) modus operandi (MO), knowledge of property fencing operations, and subsequent examinations of forensic evidence for successful investigative apprehension.

Introduction

In 2017, the UCR estimates that 1,401,840 burglaries have occurred with 841,283 occurring within a residential dwelling (255,524 during night and 424,886 during day hours) (FBI 2017). Nationally, residential burglaries accounted for 60% of all burglary offenses (FBI 2017). Notably, the probability of residential victimization is higher during summer months and during daytime hours (FBI 2017). Comparatively, commercial burglaries are more likely to be committed during night hours when businesses are closed (FBI 2017). Overall, burglaries accounted for 18.2% of the estimated number of property crimes in the USA with an estimated $3.4 billion in property losses ($2416 average loss per burglary) in 2017 (FBI 2017). Further, studies have indicated that three million individuals are victimized annually in the USA (Langton and Truman 2015).

Besides the financial losses that burglaries cost nationally, they occur in more frequency comparatively than other felonies (FBI 2017). Notably, arrest rates and victimization data are only a fraction of an indicator of burglary incidents as most are not reported, do not result in arrest, and are not included in national statistics (DeLisi et al. 2018). For example, it is estimated that only half of burglaries are actually recorded within FBI Uniform Crime Statistics with 70% of all US residences being burglarized once within a 20-year period (Osterburg and Ward 2000).

The national clearance rate for burglary is 13.5%, which includes an arrest or a clearance by exceptional means (FBI 2017). Comparatively, murder and nonnegligent manslaughter has a 61.6% clearance rate with robbery having a 29.7% clearance rate (FBI 2017). Often burglaries are difficult to investigate because solvability is dependent upon the actions of the initial responding officer(s), the efforts of crime scene technicians in processing the scene, and the subsequent investigative efforts of detective(s).

Notably, a percentage of residential burglary clearances result from indirect methods when a burglar is arrested for another offense and admits to unsolved burglaries (Mawby 2013), with most first responder activities having a direct influence upon criminal apprehension (Coupe and Griffiths 1997). Coupe and Griffiths (1997) found that first responders detaining an offender in the act or near the crime scene (43% of clearances in 256 cases) alongside effective witness/victim statements (34% of clearances) were attributed to arrest. Farrington and Lambert (2000) found that burglars were most likely to be detected being caught in the act (14%); from information from an informant (12%); apprehended near the crime scene (12%); traced through stolen property or property left at the crime scene (10%); acting suspicious in the area (8%); through a witness description (7%); and through indirect detection (7%). Comparatively, forensic evidence as the principle method of direct detection (6% of clearances in 256 cases) and subsequent CID investigations (10% of clearances) should not be discredited when investigating burglaries (Coupe and Griffiths 1997).

Therefore, all burglary investigations entail an understanding of a burglar's modus operandi (MO) or specific pattern of criminal activity, particularly vital in cases where an arrest in not made by first responding officers. Deductions toward formulating a burglar's MO can be established by drawing typological inferences about how and why a location was selected, the burglar's method of entry, the items taken/not taken, the apparent pre-commission planning involved, and how the burglar searched the property for items. Once an MO has been established, investigators can link serial burglaries together, link a suspect to previous criminal cases, and determine the individual characteristics of a burglary.

Commercial Burglars Versus Residential Burglars

Research examining burglars has shown that commercial burglaries are often preferred over residential burglaries partly because offenders can more easily justify their crimes (Mawby 2013). Mawby (2013) contends that this justification is based upon offenders' perceptions of reduced victimology (i.e., no individual victim involved) and sentencing by courts and increased profitability for commercial over residential burglary. Another

difference between commercial burglar(s) and residential burglar(s) is that target hardening (e.g., presence of security staff, dogs, etc.) may deter burglar(s) (see Kruissink 1996; Wiersma 1996). Yet, what is unique to commercial burglaries is there is often more extensive preplanning with multiple suspects taking large quantities for "orders" (Mawby 2013). An investigative focus on fencing operations could be more vital in a commercial burglary investigation than residential burglary investigations because tracking numerous objects of one type (e.g., multiple TVs) as opposed to singular items is a key feature. Comparatively, a majority of commercial burglars have previous residential burglary convictions and/or disclosed a history of residential burglaries (Mawby 2013). Hence, there is often an investigative overlap between commercial burglaries and residential burglaries.

Following an investigative blueprint, the investigations of residential and commercial burglaries are relatively similar. Investigators should examine a burglar's typology and location selection, examine their method of entry and targeted items, determine the burglar's amount of pre-commission planning, establish how the property was searched, and any post-commission acts to identify potential items of forensic and investigative value.

Burglar Typology and Location Selection

An investigation of both residential and commercial burglaries relies on determining burglar typology and selection of the target location. By determining the typology and the motivations for why a location was targeted, and offender MO can be established which aids in determining who committed the crime. Determining an MO can allow investigators to link similar cases together, link offenses to specific offenders, understand how a crime has been committed, aid in the retrieval of forensic and investigative evidence, and predict future offending patterns.

Notably, research has indicated that across commercial and residential burglary offenses, there exists variability among burglars in terms of their criminality and their criminal career (Bouhana et al. 2016; Hargreaves and Francis 2014), burglary committed with other associated crimes (Fox and Farrington 2012; Steffensmeier et al. 2015), variation in burglar motivations (Wright et al. 1995), and geographic and temporal issues in relationship to burglary (Johnson 2008). While studies indicate that skill levels vary across burglars, often the typical burglary is intersectional with other crimes focused on property crimes to support drug dependencies (Wright and Decker 1994).

Further research (Cromwell et al. 1991; Wright and Decker 1994) indicates that the selection of a burglary target is often preplanned. Burglars often have some knowledge of the items inside a residence or business along with knowledge regarding the routine of the occupants/owners. Nee and Meenaghan (2006) found 45 out of 50 UK burglars had a predictable search pattern with familiarity with the residential layout and the types of property contained within. Therefore, investigators should put CCTV footage during the course of their investigation to see if the offender can be viewed casing the location pre-commission.

Residential Burglars

Wright and Decker's (1994) study of residential burglars in Saint Louis (USA) found that they target a location based on their observations (62%) prior to commission of the crime. Further, burglars disclosed that they watched a location for some time within an area of local familiarity before committing the crime (Wright and Decker 1994). In other words, burglars target locations that are within close proximity to their normal living activities. This can include targets near their own personal residence, targets near friends/families, targets near routes to work/school, etc. Research has indicated that burglars are more likely to target locations close to their residences (Chamberlain and Boggess 2016; Rossmo 2000), often residing within a 1–2 mile radius of the actual burglary location (Bernasco 2006; Snook 2004). Therefore, investigators should interview individuals near the area of the offense to see if a suspect was casing the area pre-commission.

Uniquely, residential burglars obtain information about the target from knowing the occupant (Wright and Decker 1994). Wright and Decker (1994) found that 21% of their studied burglars target neighbors, their drug dealers, or they had jobs that brought them into targeted locations (e.g., cleaners, delivery drivers, movers, utility workers, etc.). Rarely do burglars rely upon intelligence from others (6% according to Wright and Decker 1994). Hence, it is vital that burglary investigators question neighbors about people seen in the area recently, including workers with access to the area. In business burglaries, suspicious employees or recently fired employees should be questioned (Brandl 2018). Notably, burglars will often avoid occupied locations during the commission of the crime as it reduces the probability of eyewitnesses and potential confrontation (see Coupe and Blake 2006; Goodwill and Alison 2006; Rengert and Wasilchick 2000).

Affluence cues also influence location selection. Burglars' perceptions of affluence may be based on observations of the size of the property, condition of the property, and the types of vehicles associated with the property (see Bernasco and Luykx 2003; Nee and Meenaghan 2006; Wright and Decker 1994). Burglars' observations through knowledge of expensive purchases within the residence can also affect affluence perceptions. For example, if residents dispose of a flat screen TV boxes outside of their home for garbage collection, one could easily conclude that the residents have new TVs inside their premises.

Commercial Burglars

Neighborhood familiarity affects location attractiveness for both residential and commercial burglars for several reasons. Ethnographic research has indicated that burglars favor locations in their own neighborhoods because they can blend in more easily without raising suspicion (see Rengert and Wasilchick 2000). Further, neighborhood familiarity affords burglars fewer demands upon pre-commission planning than do other unfamiliar areas (Chamberlain and Boggess 2016). Neighborhood familiarity also provides burglars knowledge of the area, knowledge of police patrol activities, and information on the people or property involved (Chamberlain and Boggess 2016; Wright and Decker 1994).

Butler (2005) found that commercial burglars appear to target larger stand-alone businesses located on the outskirts of a major town. Butler (2005) argues that commercial burglars target these businesses because the probability of apprehension is lower with police being located further away. Further, Cromwell et al. (1991) stated that commercial burglary responses might be up to 20 min to locations outside city centers that affords burglars more time to avoid apprehension. Yet, conflicting research found that inner-city neighborhoods are also more likely to be targeted because of the increased probability of the number of offenders living close to the location (Clarke 2003). In respect to the presence of security guards, they are a sight deterrence regarding commercial burglary target selection with CCTV being a potential deterrent dependent on if it is physically being monitored by security (Butler 2005).

Burglar's Method of Entry and Targeted Items

Residential Burglaries

How a burglar gains entry to a residence or business contributes to a further understanding of a suspect's modus operandi. Weisel (2004) found that two-thirds of burglaries involved forced entry through windows, doors, and back doors. Forced entry into these common entry points involved the usage of screwdrivers, crowbars, rocks, hammers, or the burglar may kick a window or door through. Weisel (2004) found that one-third of residential burglary cases involved entry through unlocked doors/windows, or open doors/windows. Often doors and windows will be checked before a burglar makes forced entry. Burglar(s) may check for uncollected mail, ring doorbells, knock on doors, or call the resident to verify occupancy pre-commission (Hakim et al. 2001; Nee and Meenaghan 2006; Palmer et al. 2002). Hence, it may be productive to dust other points of entry for fingerprints contained within the same residence/business.

Based on my professional experience as a burglary detective for several years in the USA, I observed that novice burglars were more likely to use pillowcases or bags/luggage taken from the crime scene to transport stolen items. This is why it is crucial for first responders to ask victims to describe any bags/luggage that could be used for concealment of stolen items in a police lookout. For larger items, like flat-screen TVs, often novice offenders would place garbage bags over the item during transport for concealment purposes. Hence, first responders to residential burglaries should stop suspicious individuals (those on foot and on bicycle) in the area carrying bags/luggage reported missing from the burglary, pillowcases reported missing from the burglary, and large items sticking out of garbage bags. In some cases, burglars may also steal wheelie bins during garbage collection day and store the stolen items within them for easy transport. In these cases, stopping a suspicious individual pushing a wheelie bin down the street outside garbage collection times is easily justifiable. Further, wheelie bins often have the address scribed on them, which could be connected to a burglary location during the investigation.

Besides possible containers used to transport stolen items, it is also beneficial to determine if any bicycle was taken from the victim's residence for two reasons: (1) it often indicates that the burglar has ridden the said bicycle from the incident location and arrived on foot; and (2) it aids in providing a more detailed suspect lookout for surrounding first responders. Based on my experience, burglars who steal a bicycle from the crime scene often did not arrive to the location via a vehicle. Notably, it would be rare for a bicycle to be taken by a burglar who used a vehicle post-commission of the crime.

The most common items taken during a residential burglary are things that can be easily converted to cash and easily carried away from the crime scene. For example, the most common taken items from 1,401,840 burglaries annually are currency ($1,429,781,653), jewelry ($1,362,002,838), clothing ($362,025,765), electronics ($938,765,508), and firearms ($155,186,427) (FBI 2016). Felson and Boba (2010) contended that items that are concealable, removable, valuable, enjoyable, and disposable are more likely to be taken during the commission of a burglary. Often this includes currency, jewelry, laptops, gaming consoles, iPads/tablets, etc. instead of furniture, refrigerators, washing machines, or dryers. As such, the items taken are based on the burglars' perception of value and/or their fondness of the items combined with offender mobility. Therefore, a burglar may steal beer from a fridge while leaving behind an expensive bottle of wine. Alternatively, a burglar may steal a gaming console and leave behind an expensive painting located nearby on a wall. Notably, stolen items can lead to investigative deductions, which may lead to a suspect.

Commercial Burglary

Commercial burglars' main motivation, like residential burglars, are economic in nature. Yet, commercial burglars are more likely to work in groups disabling alarms and targeting safes located inside businesses (Clarke 2003). Entry is often made in similar patterns as residential burglaries through doors and windows. Yet, 2% of commercial break-ins involved the usage of a vehicle to ram through doors or windows (see Mirlees-Black and Ross 1995).

Successful commercial burglaries, like residential burglaries, are more likely to be targeted with repeating substantial victimization due to the offender(s) gained knowledge during previous commissions. Variations in burglary risk differ among businesses due to location, premises, items sold, and security. For example, stores which are open 24 h are less likely to be targeted due to employees being present as potential witnesses, whereas a store with closing hours at night with lesser-known security measures are more likely to be targeted.

In respect to product targeting inside businesses, commercial burglars are more likely to target banks and cash registers, tobacco products, health and beauty products, electronic goods, and designer clothing (Clarke 2003). Further, research indicates that commercial burglars may target ATMs located inside businesses (see Clarke 2003).

Burglar Variances in Pre-commission Planning

Residential Burglars

Two demographic characteristics, age and gender, of burglars are associated with different pre-commission planning in both residential and commercial burglaries. Experienced burglars typically are middle-aged adults, steal highly valuable items, and commit "high-risk" burglaries (Brandl 2018). Weisel (2004) contended that experienced commercial and residential burglars are also more likely to commit offenses farther away from their homes than novice ones. Notably, experienced burglars use more advanced preplanning than do novice burglars. Experienced burglars will often bring entry tools and a bag (to carry stolen items) with them pre-commission. Experienced burglars often avoid taking aged electronic goods, instead opting for smaller and more portable electronic items, jewelry, drugs, and cash (Nee and Meenaghan 2006).

Novice burglars, on the other hand, are typically poor preplanners, stealing in a spontaneous way motivated by opportunity, fun, or excitement (Cromwell et al. 1991; Walsh 1980). Novice burglaries often involve minimal gains and often target nearby residences that do not have dogs, alarms, or locks (Brandl 2018). Further, both experienced and novice burglars prefer locations that allow them to remain unseen, such as areas with fences or natural covers that hide entry locations and building with few neighbors (Bernasco 2006; Coupe and Blake 2006; Sanders et al. 2017). As such, these types of locations reduce the probability of confrontation from a third party and/or any witnesses to the incident.

Researchers (Sanders et al. 2017) comparing residential burglaries found that male burglars are more likely than female burglars to engage in some type of intelligence planning pre-commission as the latter appear to be impulsive overall. Yet, female burglars have reported that they are more likely to be deterred by alarms, outdoor cameras, outdoor lighting, and indicators on neighborhood watches than are male burglars (Sanders et al. 2017). It is speculated that female burglars are more likely to be impulsive in the commission of burglaries because they are more involved, or motivated by, substance abuse problems than are male burglars (Sanders et al. 2017). Often women are more likely than men to take prescription narcotics from a residence. Female burglars often commit the burglary with significant others, whereas male burglars commit burglaries with friends (see Sanders et al. 2017).

Commercial Burglars

The degree of pre-commission planning for a commercial burglary may vary based on the type of location burglarized. For example, Butler (2005) found that most commercial burglars disclosed that they spent 20 min to a few hours to plan a business burglary based on security factors. Blevins et al. (2012) found in a sample of 422 convicted burglars that close proximity to other people, lack of escape routes, and indicators of increased security (alarm signs, dogs, outdoor cameras, etc.) are considered in pre-commission planning of a target. Further, 60% of burglars stated that the presence of an alarm would deter them, especially burglars who spent more time with pre-commission planning (Blevins et al. 2012). Notably, Butler (2005) contends that the amount of planning is dependent upon the professionalism of the offender. More experienced burglars are more likely to take more time with pre-commission planning to consider all the risks and factors that may influence criminal detection (Butler 2005).

Burglar's Property Search for Items

Nee and Meenaghan (2006) found that out of 50 experienced residential burglars, 45 had a predictable search pattern once inside a property that lasted under 20 min. Further, Nee and Meenaghan (2006) found that habitual residential burglars engage in a search based on what has worked in previous burglaries alongside what yields the highest gains at the lowest risk. Researchers (Nee and Meenaghan 2006; Wright and Decker 1994) found that burglars often begin their

searches in the master bedroom of a residence with the most common place searched being the kitchen followed by bathrooms (Wright and Decker 1994). Therefore, a burglar's actions during searching for property may indicate preplanning knowledge of contents of the premises (Brandl 2018). For example, a frenzied ransacking style within the crime scene is an act either of vandalism (most likely juvenile offenders) or because of poor strategic preplanning to search the premise for property (Brandl 2018). If burglar (s) have preplanning knowledge of the location of targeted items, evidence of ransacking will be minimal and the time span for the commission of the crime will be smaller. This type of preplanning can be evident within crime scenes if cabinets and drawers are left untouched and areas which contain valuables are specifically targeted. This can indicate to burglary investigators that the burglar is either a friend/family member of the victim, or a cleaner who knows where items are located in the residence. Further, the degree of ransacking is negatively associated with the relationship between the burglar and the victim (e.g., high ransacking, strangers).

Commercial burglars are more likely to visit a business prior to a burglary commission. By visiting an open business, commercial burglars can familiarize themselves with the goods and items within the targeted business and the observable security perimeters present. As such, viewing CCTV footage from several days prior to the burglary may yield an investigative lead in identifying a suspect. Further, some research indicates that commercial burglars spend less than 30 minutes inside the targeted building during the burglary (Butler 2005).

Burglary Post-commission Acts

After the burglary, burglars commit further actions that hold investigative value. Studies indicate that the main motivating factor for the commission of a burglary is to acquire cash (Palmer et al. 2002; Wright and Decker 1994). Yet, studies vary on why burglars need said cash (see Bennett and Wright 1984; Palmer et al. 2002; Wright and Decker 1994). While some burglars commit burglary for subsistence and daily expenses along with superficial factors (see Shover and Honaker 1992), often the motivation for the commission of a burglary is based on drug addiction (Hochstetler and Copes 2006; Wright and Decker 1994), particularly heroin addiction (Weisel 2004). To sell stolen items, often burglars will significantly "markdown" (Felson and Boba 2010) items to get rid of them quickly. Ferrante and Clare (2006) found that stolen goods are typically converted within hours and mostly within a day of the burglary. Felson and Boba (2010) contended that "markdowns" occur in the process of converting items to cash due to the stolen item being damaged during the burglary, as a result of being used, as a result of being stolen itself, and as a result of the burglars desire to move the item quickly.

Further, the process of turning property into cash involves varying levels of risk and effort for burglars with investigative possibilities for investigators to follow-up on (see Chart 1 below). Wright and Decker (1994) contended that stolen property is often converted within hours of the commission of the crime. As indicated in the Chart 1 below from Brandl (2018), stolen items

Method	Effort Level	Reward Level	Risk Level of Arrest
Sell stolen items to friend	Low	Low	Low
Trade for drugs	Low	Low	Low
Sell to a fencing operation	Moderate	Moderate	Moderate
Sell to a pawnshop	Moderate	Moderate	High
Sell to strangers	High	High	High

Investigations: Burglary, Chart 1 Methods of converting stolen items from burglaries versus effort and risk (Brandl 2018)

are more easily executed with a low level of risk when items are traded for drugs. Therefore, burglary investigations often coincide with narcotic investigations as it is not uncommon to execute unrelated narcotic warrants and recover stolen items taken from previous burglaries in the area.

Physical Evidence Located and the Burglary Scene

Often a search of physical evidence at a crime scene will require assistance from the victim to determine which items have been left behind, touched, or moved during the commission of the burglary. Overlooked physical evidence within burglary crime scenes are tool marks, discarded cigarettes, matchbooks, and fingerprints/footprints outside points of entry. Determining the path of burglar(s) through a residence or business is vital in the recovery of forensic evidence during the establishment of an MO. Forensic efforts should be concentrated in locations where it can be determined that the suspect(s) touched during the commission of the offense. During this search for forensic evidence, a common approach path should be taken by investigators and forensic technicians alike to reduce the likelihood of crime scene contamination. Often, departments may not have available forensic personnel and the first responder and investigator may be tasked with processing the crime scene themselves. This processing involves taking relevant photos, dusting locations for fingerprints, recording items and serial number for documentation, and subsequent follow-up of any items of investigative value.

Notably latent print recoveries are more probable during burglary investigations because burglar(s) search and touch items while looking for items of value. Additional areas that should also be examined for latent prints include contents within refrigerators as the burglar(s) may have taken food; any discarded beer/soda cans; toilet seats if the restroom has been used; etc. Suspected prints should be dusted according to department protocol and a chain of custody which documents who processed the prints alongside the recovered location should be upheld at all times to avoid contamination.

Based on my investigative experience, prints can often be found on the bottoms of dresser drawers that have been removed for searching. I also observed that when it rains and is cold, socks drawers specifically are more likely to be searched as the burglar(s) steal dry socks. In this scenario, a burglar will leave behind their wet dirty socks nearby. This modus operandi can aid investigators in concluding the suspect arrived and left the scene via foot instead of a vehicle.

Besides the recovery location of latent prints inside a crime scene and the linkage to a burglar (s) modus operandi, the advancement of the Automated Fingerprint Identification System (AFIS) is valuable in burglary investigations. AFIS technologies allow for recovered latent prints to be compared to the prints electronically archived in criminal records. By using ridge endings and bifurcations contained within criminal record fingerprint files, digitalized representation of fingerprints can be stored and then compared to digitally inputted suspect fingerprints. Notably, a fingerprint examiner can only verify an official fingerprint match manually as the AFIS system only narrows down a potential suspect sample. As there are 90+ unique identification points on each finger, even partial prints may be run on AFIS (Osterburg and Ward 2000). Notably, at least 13+ identifiable points are needed for an identification in the USA; comparatively, France requires 17 points of reference and England requires 13 points of reference for identification (Osterburg and Ward 2000).

Besides forensic techniques that can connect burglar(s) to burglary scenes, clearance rates of burglaries often reside upon records and information about stolen property. Electronics, handguns, bicycles, and other items have unique identification numbers. Therefore, if a victim has recorded and documented unique serial numbers they can be compared to pawn system databases, National Crime Information Center (NCIC) databases, items founded in narcotics warrants, and items recovered in other crime scene locations. By

having comparative record numbers, the burglary can be effectively prosecuted. Often, a suspect will not face prosecution if there is nothing unique or identifiable about a stolen item. Currently, there exist no formal stats on the success rate of the recovery of stolen items with serial numbers, yet when examining FBI statistics, recovered items documented are more likely to have a higher probability of formally recorded serial numbers (e.g., vehicles, handguns, large office equipment, large electronics).

Further, a specific lookout can be placed for any stolen material with a known unique identification number on NCIC, which is used nationally to trace items by law enforcement. If items with a known unique identification number are taken, the odds of successful investigative recovery are greatly increased. Hence, it is vital that both businesses and residents document the serial numbers of valuable items. Notably, if a suspect is stopped after the commission of a burglary and is in possession of similar items taken from a burglary without identification number verification, it could not be judiciary concluded that said items are the same as those burglarized.

Conclusion

During a burglary investigation, the establishment of a modus operandi can identify an offender and provide the basis for apprehension. Further, the establishment of a modus operandi in a burglary investigation can link serial burglaries together and link a suspect to previous criminal cases. Possessing a better understanding of empirical studies of burglars, burglar crime analysis, burglar crime commission, and post-commission actions can aid investigators in narrowing their search for physical evidence within a crime scene. For example, having a better knowledge of a burglar's MO may aid in determining potential latent print locations within a residence/business. Further, the successful recovery of "readable," identifiable prints may assist in identifying a burglar (if their prints are on AFIS). Besides offender identification and typology in burglary investigations, the conversion of stolen property with unique identification numbers can additionally aid in apprehension of suspect(s) and the recovery of stolen items. Therefore, there are several possibilities that investigators can explore in conducting a burglary investigation from their interaction with first responders; to an adequate immediate search for suspect(s); to effective questioning of witnesses; to the successful processing of a scene; and to the subsequent examination of traceable items with unique identification numbers on NCIC.

Cross-References

- ▶ Arrest
- ▶ Criminals: Motives
- ▶ First Responders: Police
- ▶ Investigations: Criminal
- ▶ Investigations: Use of DNA and Fingerprints

References

Bennett, T., & Wright, R. (1984). *Burglars on burglary: Prevention and the offender*. Hampshire: Gower.

Bernasco, W. (2006). Co-offending and the choice of target areas in burglary. *Journal of Investigative Psychology and Offender Profiling, 3*, 139–155.

Bernasco, W., & Luykx, F. (2003). Effects of attractiveness, opportunity and accessibility to burglars on residential burglary rates of urban neighborhoods. *Criminology, 41*(3), 981–1002.

Blevins, K. R., Kuhns, J., & Lee, S. (2012). Understanding decisions to burglarize from the offender's perspective. The University of North Carolina at Charlotte, Department of Criminal Justice & Criminology. Retrieved December 1, 2018, from http://airef.org/research/BurglarSurveyStudyFinalReport.pdf

Bouhana, N., Johnson, S. D., & Porter, M. (2016). Consistency and specificity in burglars who commit prolific residential burglary: Testing the core assumptions underpinning behavioural crime linkage. *Legal and Criminological Psychology, 21*(1), 77–94.

Brandl, S. G. (2018). *Criminal investigation*. London: Sage.

Butler, G. (2005). Commercial burglary: What offenders say. In *Crime at work* (pp. 29–41). London: Palgrave Macmillan.

Chamberlain, A., & Boggess, L. (2016). Relative difference and burglary location: Can ecological

characteristics of a burglar's home neighborhood predict offense location? *Journal of Research in Crime and Delinquency, 53*(6), 872–906.

Clarke, R. (2003). Burglary of retail establishments. Center for Problem-Oriented Policing. Retrieved December 1, 2018, from https://popcenter.asu.edu/content/burglary-retail-establishments.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology, 44*, 431–464.

Coupe, T., & Griffiths, M. (1997). *Solving residential burglary* (Crime detection and prevention series, paper no. 7). London: Home Office.

Cromwell, P. F., Olson, J. N., & Avary, D.'. A. W. (1991). *Breaking and entering: An ethnographic analysis of burglary* (Vol. 8). Newbury Park: Sage.

DeLisi, M., Nelson, E. J., Vaughn, M. G., Boutwell, B. B., & Salas-Wright, C. P. (2018). An epidemiological study of burglary offenders: Trends and predictors of self-reported arrests for burglary in the United States, 2002–2013. *International Journal of Offender Therapy and Comparative Criminology, 62*(4), 1107–1127.

Farrington, D., & Lambert, S. (2000). Statistical approaches to offender profiling. In D. Canter & L. Alison (Eds.), *Profiling property crimes* (pp. 233–273). Aldershot: Dartmouth.

Federal Bureau of Investigation. (2016). *Uniform crime reporting program data: Property stolen and recovered, United States, 2016*. Ann Arbor: Inter-University Consortium for Political and Social Research [distributor], 2018-07-19. Retrieved December 1, 2018, from https://doi.org/10.3886/ICPSR37063.v1.

Federal Bureau of Investigation. (2017). Uniform crime report: Crime in the United States, 2017. Retrieved December 1, 2018, from https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/burglary

Felson, M., & Boba, R. L. (2010). *Crime and everyday life*. London: Sage.

Ferrante, A., & Clare, J. (2006). *"Known" burglars and the stolen goods market in western Australia (research report)*. Perth: Office of Crime Prevention, Western Australian Department of Premier and Cabinet.

Fox, B. H., & Farrington, D. P. (2012). Creating burglary profiles using latent class analysis: A new approach to offender profiling. *Criminal Justice and Behavior, 39*(12), 1582–1611.

Goodwill, A. M., & Alison, L. J. (2006). The development of a filter model for prioritising suspects in burglary offences. *Psychology, Crime & Law, 12*(4), 395–416.

Hakim, S., Rengert, G. F., & Shachmurove, Y. (2001). Target search of burglars: A revised economic model. *Papers in Regional Science, 80*(2), 121–137.

Hargreaves, C., & Francis, B. (2014). The long term recidivism risk of young sexual offenders in England and Wales – Enduring risk or redemption? *Journal of Criminal Justice, 42*(2), 164–172.

Hochstetler, A., & Copes, H. (2006). Opportunities and decisions: Interactional dynamics in robbery and burglary groups. *Criminology, 39*, 737–763.

Johnson, S. D. (2008). Repeat burglary victimisation: A tale of two theories. *Journal of Experimental Criminology, 4*(3), 215–240.

Kruissink, M. (1996). Commercial burglary: The offender's perspective. *Security Journal, 3*(7), 197–203.

Langton, L., & Truman, J. (2015). *Criminal victimization, 2014*. Washington, DC: Bureau of Justice Statistics, US Department of Justice.

Mawby, R. (2013). *Burglary*. London: Routledge.

Mirlees-Black, C., & Ross, A. (1995). *Crime against retail and manufacturing premises: Findings from the 1994 commercial victimization survey. Home Office research study, no. 146.* London: Home Office.

Nee, C., & Meenaghan, A. (2006). Expert decision making in burglars. *British Journal of Criminology, 46*(5), 935–949.

Osterburg, J. W., & Ward, R. H. (2000). *Criminal investigation: A method of reconstructing the past*. Cincinnati: Anderson.

Palmer, E., Holmes, A., & Hollins, C. (2002). Investigating burglars' decisions: Factors influencing target choice, method of entry, reason for offending, repeat victimisation of a property and victim awareness. *Security Journal, 15*, 7–18.

Rengert, G., & Wasilchick, J. (2000). *Suburban burglary: A tale of two suburbs* (2nd ed.). Springfield: Charles C Thomas.

Rossmo, K. (2000). *Geographic profiling*. New York: CRC Press.

Sanders, A., Kuhns, J., & Blevins, K. (2017). Exploring and understanding differences between deliberate and impulsive male and female burglars. *Crime & Delinquency, 63*(12), 1547–1571.

Shover, N., & Honaker, D. (1992). The socially bounded decision making of persistent property offenders. *Howard Journal of Criminal Justice, 31*(4), 276–293.

Snook, B. (2004). Individual differences in distance travelled by serial burglars. *Journal of Investigative Psychology and Offender Profiling, 1*, 53–66.

Steffensmeier, D., Harris, C. T., & Painter-Davis, N. (2015). Gender and arrests for larceny, fraud, forgery, and embezzlement: Conventional or occupational property crime offenders? *Journal of Criminal Justice, 43*(3), 205–217.

Walsh, D. (1980). *Break-ins: Burglary from private houses*. London: Constable.

Weisel, D. L. (2004). *Burglary of single-family houses* (Problem-oriented guides for police, problem-specific guide series, no. 18). Washington, DC: US Department of Justice.

Wiersma, E. (1996). Commercial burglars in the Netherlands: Reasoning decision makers. *International Journal of Risk, Security and Crime Prevention, 1*(3), 217–225.

Wright, R., & Decker, S. (1994). *Burglars on the job: Streetlife and residential break-ins*. Boston: Northeastern University Press.

Wright, R., Logie, R. H., & Decker, S. H. (1995). Criminal expertise and offender decision making: An experimental study of the target selection process in residential burglary. *Journal of Research in Crime and Delinquency, 32*(1), 39–53.

Further Reading

Brandl, S. G. (2018). *Criminal investigation*. Thousand Oaks: Sage.

Mawby, R. (2013). *Burglary*. London: Routledge.

Pogrebin, M. (Ed.). (2011). *About criminals: A view of the offenders' world*. London: Sage.

Investigations: Consumer Retail Shoplifting

Trevor A. Smith
University of the West Indies, Mona, Jamaica

Keywords

Retail shoplifting · Retail theft · Shop theft · Shrinkage · Concealed goods

Definition

Consumer retail shoplifting, also referred to as retail theft and shop theft, can be defined as the stealing of consumer goods from a retail outlet. This act of larceny/theft, i.e., intentionally and unlawfully taking possession of the property of another, is usually classified as shoplifting when it is done by the shopper or people pretending to be shopping during the opening hours of the store. If the shopper leaves the outlet and forgets to pay for the goods, then this would not be considered as shoplifting as the element of intention is missing.

Introduction

The scholarly work on shoplifting is largely located within the disciplines of criminology and consumer behavior with many of the studies done on the characteristics of the shoplifter, causes of the behavior, shoplifting prevention strategies, and consequences (or lack thereof) of engaging in the act of shoplifting. This phenomenon continues to have a significant and negative impact on the retail business industry despite the enactment of civil shoplifting statutes aimed at mitigating this problem in countries such as the United States. These statutes permit the retailer to recover damages and enforce penalties against the culpable shoplifter.

As the economy gets tight, shoplifting is expected to increase as people will find a way to satisfy their needs and desires. As such, the retail business form will naturally lose money due to shrinkage. The term shrinkage refers to the unexplained loss in inventory due to theft, shoplifting, errors, and fraud (National Retail Federation 2018) with shoplifting being the largest source of these lost revenues (Du and Maki 2019).

The large majority of shoppers have stolen from retail stores at some time during their lives. And while this is *eye-opening*, it is unfathomable to conclude that most of these people are criminals (Cox et al. 1990). That said, only 1 in 11 shoppers is engaged in shoplifting on a regular basis (Blanco et al. 2008), and 1 in 150 shoplifters is apprehended by the police (Farrington 1999). Police data on shoplifting is problematic as only a small portion of the crime is reported (ONS 2014), and the percentage of shoplifters who get caught is very small.

The act of shoplifting is usually committed by shoppers or people pretending to be shopping and involves the concealing of the items and leaving the store without paying for these items. Other forms of shoplifting would include fake refund, switching of price tag and paying the lower price, and eating of food in grocery stores without making payment. Fake refund does not involve the direct stealing of an item but rather the illegal taking of a cash refund for goods from a store where the goods were not purchased. There is also the notion of digital shoplifting where people illegally photograph materials from books for reading later.

Retail theft can be committed at any time but is usually at its lowest in the early mornings and highest in the early evenings (Bamfield 2012). It has been said that shoplifting is more popularly committed during busy periods like public holidays and stores are more vulnerable at times such as just after opening, just before closing, and during shift changes. Moreover, retail theft is most likely to happen when sales staff are

occupied or distracted. These offenders will try to distract store personnel by asking questions that will lead the staff away from their stations thus giving the perpetrator enough time to make the move. For example, questions about out of stock items could lead the store personnel to the warehouse or to the back of the store and leaving the shoplifter with wiggle room to commit the act. Product categories that are popularly shoplifted include electronics, cosmetics, and clothing.

The layout of the modern retail concept is very accommodating to the shoplifter as holding areas for stealing goods are facilitated through shelves, spaces, and secluded areas within these stores. Goods that are shoplifted are then concealed in pockets, coats, oversized clothing, handbags, and backpacks – a favorite carrier among petty thieves for hiding stolen items. There is also the case where shoplifters will conceal goods such as clothing or a wristwatch by wearing the item in plain sight when leaving the store. Some shoplifters will even purchase one item to conceal another in the packaging.

The fitting room area is also a popular space to conceal goods. In this area, the shoplifter will pack bags with stolen items, switch tags with cheaper ones, and bring a lot of clothing items in dressing rooms so that sales representatives cannot be certain of what is taken and what is left behind. The shoplifter will try to make a speedy exit when in possession of the stolen items. However, this is not usually done by running away from the scene but by walking away briskly so as not to attract attention. Store employees should therefore be proactive and look out for these suspected personalities as they can often be found loitering in the stores, showing signs of excessive sweating, fidgeting, and displaying other nervous-type behaviors.

The motivation for shoplifting is not fully understood as the large majority of shoplifters indicate that there was no plan or intention to steal before entering the store which therefore suggests that shoplifting may be due to stimulus-response, i.e., an impulsive behavior in large measures and not to criminal intent. Most shoplifters are therefore amateurs and not professional thieves. Amateurs usually steal on impulse for personal use and utilized methods that are crude and simple. These people do not consider themselves as criminals and are often distraught when described in such terms. When caught and subsequently arrested, these amateurs will often express disbelief when treated as criminals. The professionals, on the other hand, are usually skillful and habitual thieves with criminal intent and may steal on their own or may utilize a ring of criminals to steal and sell for making profits. These professional thieves utilized methods that are carefully orchestrated and are usually knowledgeable about the shop layout, knowing what they want and where to get it. Taylor (2011) described three scenarios involving techniques that are utilized by professional shoplifters (Table 1).

The cost of shoplifting is borne by the honest consumer as the practice is to offset the retail losses by increasing the price to consumers. However, if the competition makes it

Investigations: Consumer Retail Shoplifting, Table 1 Techniques utilized by professional shoplifters

1. Booster Box
• Shoplifter enters store with large box on trolley.
• Box has identifiable image, such as a large television, with tag from another store displayed.
• Box is empty on entering but looks full, with visible packaging tapes around it.
• Box is then filled with shoplifted goods from underneath and tape affixed at the bottom to ensure goods do not fall out.
• Shoplifter then leaves the store with box on trolley and is not challenged by store personnel as product is clearly identified as being bought elsewhere.
2. Double Docketing
• Shoplifter loads two trolleys with same or similar items then and goes to cashier with one trolley with the other left behind.
• Shoplifter then pays for goods, collects receipt, exits store, and unpacks goods.
• Shoplifter then reenters store, picks up the other trolley with an additional item, returns to same cashier, pays for item, produces previous receipt, and explains to cashier that item was forgotten and returning in line was merely to pay for the additional item.
• Shoplifter then exits store with other trolley.
3. Distraction
• At least two people who are working together enter the store.
• One party distracts store attendant, and the other party takes goods and exits store.

infeasible to increase prices, then the retailer will have to absorb the losses. And even though retailers are under pressure from consumers to reduce prices, many retailers will not allocate the necessary resources to combat the shoplifting problem as there are so many competing needs for the limited resources. Moreover, most retailers do not have the will to combat shoplifting as detection and prosecution take time and energy and the mistaken apprehension of shoppers may result in costly lawsuits. Further, stores could acquire a bad reputation of crime if shoplifting were to be reported regularly (Clarke and Petrossian 2003). Shrink is estimated to cost retailers 1.33% of sales in the United States (National Retail Federation 2018) and US$400 per shopper on an annual basis (Brickhouse Security 2015).

Classifications of Shoplifters

Shoplifting is widespread and is one of the most prevalent forms of criminal activity. These offenders can be found among all ages, sexes, and economic and ethnic groups. There are reports that suggest that shoplifting may even be prevalent among high-income and highly educated individuals (Blanco et al. 2008). As such, shoplifters cannot be easily identified based on demographic variables. Hence, we must seek to uncover other classifications if the business is to effectively identify these offenders.

There are at least two broad classifications of shoplifters – economic and psychosocial. Economic motivators are displayed by individuals who take part in these activities for profits, while psychosocial motivators are more complex and are driven by dispositions such as peer pressure, impulsiveness, excitement, low self-esteem, stress, and compulsion. Thus, shoplifting is often triggered by need for financial gains along with a variety of psychosocial issues that are experienced by people who are otherwise law-abiding. The perpetrators of shoplifting could also be classified into groups such as professionals, kleptomaniacs, drug abusers, poverty stricken, and excitement seekers. See Table 2.

Investigations: Consumer Retail Shoplifting, Table 2 Classification of shoplifters

• **Professionals** – habitual stealing for profiting in a natural course of living
• **Kleptomaniacs** – inability to contain the urge for stealing and typically done for reasons other than personal use or financial gain
• **Drug abusers** – steal to maintain drug habits
• **Poverty stricken** – steal because of need of basic items
• **Excitement seekers** – steal because of the thrill from excitement caused by the adrenalin rush

Identifying the Shoplifter

It may be difficult to pinpoint who exactly will shoplift as this question is confounded by so many factors and reasons. Some of the reasons for committing this crime include necessity, desperation, desire of luxury items that offenders cannot afford, and psychological diseases such as kleptomania and other compulsive disorders. Thus, shoplifting is a complex behavioral issue that has no easily defined template for identifying the offender. Moreover, it is difficult to ascertain what the shoplifter looks like since there are no distinct physical traits as these perpetrators are likely to be male or female of any race or ethnicity and may be rich or poor (Pilon 2019). Notwithstanding this complex problem, in the identification of the shoplifter, there are many telltale behavioral cues that the retailer must utilize. The more typical signs and signals are summarized in Table 3.

Some of these behavioral types can be found among honest shoppers in the course of doing their shopping. However, these telltale signs and signals, while not exhaustive, provide a basic *snapshot* of the expected behaviors among shoplifters.

Preventing Shoplifting

High-value goods placed at the entrance of retail stores are known to attract patrons into these stores and at the same time provide easier access to shoplifters to grab and run away with the goods.

Investigations: Consumer Retail Shoplifting, Table 3 Signs and signals of the shoplifter

• Frequent users of washrooms
• Entering stores with large numbers of bags and bundles
• Wearing large and out of season clothing
• Leaving store in a hurry
• Moving in an unusual manner
• Loitering in the store
• Showing signs of excessive sweating, fidgeting, and other nervous-type behaviors
• Regularly picking up and putting down items

Investigations: Consumer Retail Shoplifting, Table 4 Shoplifting prevention strategies

• Increase the number and visibility of uniform security guards
• Utilize plainclothes store detectives
• Use security personnel to patrol aisles in store
• Redesign store layout to have a bird's-eye view of all areas
• Limit the number of changing rooms in clothing department and have sales person take inventory of the items entering and leaving the changing room
• Keep bags for shoppers on entering and returning them on leaving store
• Limit the number of exits from store
• Position cashiers in close proximity to store exit
• Install closed-circuit television (CCTV) monitoring and convex mirrors
• Install radio-frequency identification (RFID) anti-shoplifting technology
• Lock away small, expensive, and popular items in showcase
• Affix expensive items to shelves or clothing racks
• Utilize split-apart labels which will pull apart with attempts to remove
• Use large packaging for small item, making more difficult to hide
• Install facial recognition technology
• Post deterrence signs in strategic areas
• Utilize merchandising tags with sensors and sound alarms
• Participate in at-risk-youth programs with police and schools
• Check the purchase against the receipt
• Provide employee training on awareness, detection, and prevention strategies

This presents a problem for the retailer as the showcasing of goods in conspicuous spaces is a tried and proven practice for attracting customers to retail outlets. The challenge of the retailer therefore is to keep shoplifting at a minimum if not totally eradicated. However, the store is faced with the dilemma of deciding how much of the goods to display as it is generally agreed that the more goods that are openly displayed, the more is the likelihood of increasing sales and inciting shoplifters. To address this dilemma, the entity must embark on a loss prevention strategy.

In rolling out this strategy, it is important to measure the extent of the shoplifting problem. This is usually measured using the ratio of the shoplifting loss to sales. Small retailers may have more difficulty to establish the levels of shrink as they are not able to acquire elaborate inventory management systems. This initial size-up of the problem is done to establish a baseline for comparing shoplifting losses before and after the preventative intervention. The prevention strategy should then be monitored and evaluated to determine the effectiveness of the shoplifting intervention. Some of the practical intervention strategies utilized by retailers are summarized in Table 4.

Retailers are now using technologically advanced methods such as cyber and analytics to prevent shrink. Investigative experience, employee integrity screening, and loss prevention awareness programs are also utilized to curtail this problem.

Even though employees are often trained to exercise vigilance in the direct confrontation with shoplifters, this is a risky strategy as these employees could be harmed by violent perpetrators. Many retail outlets have therefore advised employees to limit direct confrontation with shoplifters to verbal exchanges and not to be physically engaged in apprehending these offenders. Some of these strategies such as checking of the shopper's bags and searching of the person may not be legal in some jurisdiction without probable cause.

Other soft but effective strategies that retailers can utilize to discourage shoplifters are to approach each customer with a sense of immediacy, always greeting customers, offering to help them to find what they are looking for, and never leaving the vulnerable points in the store unattended. Greeting customers on entering the store is not only for the purposes of courtesy and

customer service but to signal to the would-be shoplifters that they are on the radar of the retailer. This simple intervention may lead to rethinking and changing of the mind of the potential shoplifter. With the effective execution of this suite of strategies, the would-be offender will certainly realize that this is not the time and place to steal. The onus is therefore on the retailer to implement and monitor shoplifting prevention strategies to mitigate this crime.

Is Shoplifting a Lesser Crime?

The act of shoplifting is not to be confused with burglary or robbery since burglary refers to the unlawful entry into a building with the intention to steal while robbery is defined as the unlawful taking of property using force or the threat of force. In most jurisdictions, shoplifting is prosecuted under larceny which has two categories – grand larceny, a felony associated with a higher dollar value of goods stolen, and petty larceny, a misdemeanor associated with a lower dollar value stolen. These dollar values may vary from one jurisdiction to the other. In the strictest sense, shoplifting could be classified as felony or misdemeanor depending on the dollar value of goods stolen. Nonetheless, it is the view of the typical shoplifter that the financial benefit derived from the act far outweighs the risk and the associated penalty is seen by these shoplifters as a *slap on the wrist*, at worst. This notion was highlighted by Solomon and Ray (1984) in the eight common beliefs of the shoplifter. See Table 5.

Investigations: Consumer Retail Shoplifting, Table 5 Eight common belief of shoplifters

- I will not get caught if I am careful and smart
- I will not be turned in and prosecuted even if I get caught
- The punishment will not be severe even if I am prosecuted
- The merchants deserve what they get
- It is OK for me to do so as everyone does it at some time or another
- This is not a major crime
- The items that I shoplift are the items I want
- The merchant expects me to shoplift

Offenders seem to have less inhibitions in stealing from shops, a property crime, than from stealing from private individuals, an offense against the person, as they believe there are less chances of being caught with shoplifting, and if caught, there are much less consequences as they can get away with plausible excuses such as forgetting to pay (Clarke and Petrossian 2003). These common beliefs of the shoplifters demonstrate a maladaptive way of thinking and lack of moral concern among this group.

Some observers such as Elder (1989) and Klemke (1992) have suggested that this act of larceny is not perceived as a serious crime by society; and others, such as Brodsky et al. (1981) and Kraut (1976), have even referred to the act as a *folk crime*, thus alluding to the trivial way that the crime is often treated. There is also the view among some retailers that the criminal justice system does not treat the crime seriously as the cases are given low priorities and many convictions have resulted in cautions (Bamfield 1997). In general, crime against property, such as shoplifting, is not viewed as seriously as crime against the person, and police charges are often downgraded on these crimes.

For a conviction of shoplifting, the act (*actus reus*) of shop theft must take place, and the person so accused must possess the intention (*mens rea*) to commit such crime. In actuality, the penalties of shoplifting (if convicted) are usually less than other larceny crimes and are usually up to the judge's discretion in most jurisdictions. It is not uncommon therefore, particularly for first-time offenders, for the penalty of shoplifting to simply be *to return the stolen goods*, *pay for the goods*, or these perpetrators may just be given a *reprimand and warning*. Notably, shoplifters do not usually commit other crimes and are not perceived as criminals by many people.

Taking Action Against the Shoplifter

The management of the store should utilize a systematic approach for taking action against the shoplifter. First, when shoplifting is suspected by the security or employees of the store, the store

management should be contacted speedily for the necessary actions to be taken. Second, the suspected offender(s) should be allowed to exit the store before any detention is made as the accosting of a perceived customer within the store may send negative signals to other customers, who, as a result, may decide not to further shop at that store. Third, the suspect should be invited to a private space in the presence of the manager aimed at resolving the discrepancy, making effort not to accuse the suspect of theft during the detention. Notably, a false accusation could result in an expensive lawsuit. Fourth, the police should only be called on reasonable suspicion of shoplifting. That is, the police should not to be called on trivial matters as this could lead to the *cry wolf* syndrome with the effect that the retailer is not believed by the police when help is really needed.

Conclusion

The act of consumer retail shoplifting is perhaps the most prevalent form of criminal activity. This is because a large proportion of the population has stolen from a retail store at some time or the other. This activity has a negative multiplier effect on the economy and should be viewed as a significant menace to society. In effect, it contributes to the shrinkage losses of the retailer, increases the price to consumers, reduces taxation revenues to government, and increases the case burden on the court system.

Retailers must therefore be proactive in preventing shoplifters from concealing their goods in pockets, bags, and clothes since many of these goods may not have the alarm devices affixed, and so concealment provides an easy path to stealing. The active monitoring of cameras will also go a far way in resolving this concealment issue as shoplifters will never feel safe when they know that they are being watched. Further, several staff positions in retail outlets, such as cleaners and shelf packers, will be engaged in work before stores are open and after they are closed. This is usually done in preparation for opening the store. In order to add another layer of monitoring, the work rosters of these stores could be redesigned to allow enough staff to work during opening hours – the time that defines shoplifting. In that way, there will always be an attendant in place to *blow the whistle.* Greeting of shoppers on entering the store and helping them to find what they are looking for could also signal to potential shoplifters that they are being monitored.

In the final analysis, it is difficult to pinpoint the shoplifter based on appearance as these perpetrators can be found across all demographic and behavioral types. And while there are many telltale signs and signals that will help in the identification of the shoplifter, these indicators are often not reliable. Security personnel within these retail stores, while not ignoring telltale signs and signals, should continue to focus attention on large handbags, coats, and oversized clothing as concealment can hardly be successful without these carriers.

Cross-References

- ▶ Investigations: Employee Theft of Employer Property
- ▶ Retail Security: Shoplifting
- ▶ Retail Security: Use of Security Guards

References

Bamfield, J. (1997). *Making shoplifters pay: Retail civil recovery.* London: The Social Market Foundation.

Bamfield, J. A. (2012). Shopping and crime. In *Shopping and crime* (pp. 1–10). London: Palgrave Macmillan.

Blanco, C., Grant, J., Petry, N. M., Simpson, H. B., Alegria, A., Liu, S. M., & Hasin, D. (2008). Prevalence and correlates of shoplifting in the United States: Results from the National Epidemiologic Survey on Alcohol and Related Conditions (NESARC). *American Journal of Psychiatry, 165*(7), 905–913.

Brickhouse Security. (2015). Costly loss prevention mistakes. https://www.brickhousesecurity.com/product_images/uploaded_images/5costly-loss-prevention-mistakes-whitepaper.pdf. Retrieved on October 11, 2019.

Brodsky, S. L., Bematz, M. L., & Beidleman, W. B. (1981). The perfect crime. *British Journal of Criminology, 21*, 350–353.
Clarke, R. V. G., & Petrossian, G. (2003). *Shoplifting*. US Department of Justice, Office of community oriented policing services.
Cox, D., Cox, A. D., & Moschis, G. P. (1990). When consumer behavior goes bad: An investigation of adolescent shoplifting. *Journal of Consumer Research, 17*(2), 149–159.
Du, L., & Maki, A. (2019). These cameras can spot shoplifters even before they steal. *Bloomberg News*, March 4, 2019, 10:00 AM EST Updated on March 4, 2019, 6:38 PM EST.
Elder, A. (1989). Retail theft: The hidden crime. *Retail and Distribution Management, 17*(3), 39–41.
Farrington, D. P. (1999). Measuring, explaining and preventing shoplifting: A review of British research. *Security Journal, 12*(1), 9–27.
Klemke, L. W. (1992). *The sociology of shoplifting: Boosters and snitches today* (pp. 7–9). Westport, CT: Praeger.
Kraut, R. E. (1976). Deterrent and definitional influences on shoplifting. *Social Problems, 23*(3), 358–368.
National Retail Federation. (2018). National Retail Security Survey, https://cdn.nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf. Retrieved on October 11, 2019.
Office for National Statistics (ONS). (2014). *Crime in England and Wales, year ending March 2014*. London: ONS.
Pilon, A. (2019). 25 Signs of a shoplifter in your store last updated: Feb 18, 2019 by Annie Pilon In Retail Trends, https://smallbiztrends.com/2019/01/signs-of-a-shoplifter.html. Retrieved on January 1, 2020.
Solomon, G. S., & Ray, J. B. (1984). Irrational beliefs of shoplifters. *Journal of Clinical Psychology, 40*(4), 1075–1077.
Taylor, M. (2011, June 20). What does a shoplifter look like? Group 1 Security, business – Security and loss prevention. *Retail World*. http://group1security.com.au/uploads/files/What%20does%20a%20shoplifter%20look%20like.pdf. Retrieved on October 28, 2019.

Further Reading

Business Still Booming for One Industry: Shoplifting, *The Washington Times* (Washington, DC); May 11, 2009; Harper, Jennifer.
Shapiro, L. R., & Maras, M.-H. (Eds.). (2019). *Encyclopedia of Security and Emergency Management*. Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-319-69891-5_56-3.
Shoplifting rises in U.S. as the economy drops, International Herald Tribune; December 24, 2008; Ian Urbina and Sean D. Hamill The New York Times Media Group.

Investigations: Criminal

Brian Kohlhepp
John Jay College of Criminal Justice, New York, NY, USA
Detective Sergeant, Ross Township Police, Pittsburgh, PA, USA

Keywords
Robbery · Burglary · Rape · Sex assault · Murder · Homicide · Interview · Interrogation · Evidence · Crime scene · Trial · Prosecution

Definition

Criminal investigations involve systematic series of actions by an investigator, guided by the penal code for a jurisdiction in which the crime occurred, that uncover or make available facts that could be used to identify, locate, and prosecute a suspect (e.g., prove guilt).

Introduction

A complete criminal investigation includes searching, interviews, interrogations, evidence collection and preservation, and various methods of investigation (Woods 2013). The steps involved are governed by penal codes that involve an overlapping system of governments and the legislated laws pertaining to their areas of responsibility (Nemeth 2018). This layering begins with local government that includes the city, township, county, or municipality. In more urban areas, the municipal government may have layers of both a local and county government, but these entities legislate through ordinances that generally regulate behavior of very minor offenses and are often more concerned with building code and regulations than criminal offenses.

The next layer is legislating criminal behavior by the state of providence. In this realm is where

the bulk of criminal behavior is codified as there is a vast array of offenses from the state or provincial government (Nemeth 2018). These statutes become categorized by offenses based upon the seriousness of which the action is considered. Most jurisdictions divide these crimes into three basic categories – summary, misdemeanor, and felony (Nemeth 2018). Summary offenses (e.g., public drunkenness, harassment, vandalism) are the lowest level of criminality and generally require very little investigation to determine the offense and the individual who perpetrated it. Misdemeanor offenses (e.g., fraud, theft, minor assaults) are behaviors conceived as contrary to public good or as producing increased suffering by the victim. Felonies (e.g., murder, rape, burglary) are considered the highest level of offense and the most serious against the public good.

The last layer of government is the federal or national law. This involves offenses legislated by the federal government as criminal behavior (Nemeth 2018). Often this level is relegated to offenses against the federal government or large sections of the populace (e.g., treason, terrorism). However, many federal governments have passed laws regulating individual behavior for offenses that are either especially heinous or which require federal resources to supplement the complex investigations. These include crimes such as child pornography, serious drug crimes (e.g., drug trafficking, sale of illicit street drugs), kidnapping, and bank robbery in the United States because banks are federally insured. White-collar crime and corrupt organizations can likewise invoke federal jurisdiction. These laws are used to investigate and prosecute organized crime rings, such as the mafia and street gangs. The federal laws and law enforcement agencies can also become involved if the crime involves multiple jurisdictions, such as occurs when criminals cross state or provincial lines (Nemeth 2018).

A criminal investigation starts with determining if a crime was committed and then seeking to determine who most likely committed this crime. The evidence that is gathered by the investigator helps to indicate suspicion of a specific person or people. The investigator will usually attempt to determine which individuals had the "means, motive, and opportunity to commit the crime" and to establish the relationships between the victim and any known offenders (Burgess, Roberts, and Rehehr 2009). Often people are victimized by someone they know either intimately or at least moderately.

The type of crime (i.e., crimes against persons, crimes against property, crimes against society) affects the degree of effort and amount of time involved to perform the investigation and typically is consistent with the grading of offenses discussed above (Nemeth 2018). Crimes against persons are defined as crimes in which a specific person has been victimized in the commission of the offense (e.g., criminal homicide, sexual assaults, and robberies). Property crimes, although they do not involve the body or a person being specifically victimized in terms of bodily harm, are nonetheless not victimless. In these crimes it is the property of the victim that is targeted (e.g., theft, embezzlement, burglary). Crimes against society refer to acts that disrupt civil life and/or violate the norms and values of society (e.g., prostitution, illegal gambling, an illegal drug use). The delimitation of these offenses differs in the grading and seriousness of the offense, as well as in the way they are investigated.

The majority of criminal offenses, or suspected criminal offenses, are investigated by a law enforcement agency that is the extension of an executive branch of government (Nemeth 2018). Correspondingly, there are dedicated and trained people possessing the equipment, resources, and training to assist in all aspects of the investigation. However, often these duties fall to private investigative entities (Nemeth 2018). This can occur for a number of reasons. For instance, a law enforcement agency may take the position that there was no offense (or minimal evidence) that violated the criminal code and therefore there is no point in wasting efforts or resources in this pursuit. A victim, family of a victim, or entity may feel otherwise and hire private agents to begin an investigation with the eventual goal of persuading the law enforcement entity that there was a criminal violation. In contrast, a large institution may be the victim of a crime against property that the company

does not want to make public. The company may prefer to have the incident investigated privately so that it may act to remove violators and remedy the situation quietly and without public notice. Once a government agency is involved, paperwork filed through the judicial branch can be publicly available, and the situation may be learned by the news media or those with a specific interest in this entity or its business. This rest of this entry describes various methods used to gather evidence in civil and criminal investigations and explains elements involved in investigations of crimes against persons, crimes against property, and crimes against society performed by a private entity.

Evidence Gathering in Investigations

There are two types of evidence – testimonial and physical – which investigators use to prove or disprove facts in contention. Testimonial evidence involves a statement by a person who is a witness to an act or one that provides information concerning the incident being explored. Examples of this would be an "eye" or "ear" witness to an event related to the incident in question. It could also be a person who was given information by a person under investigation, such as suspect providing a confession. Physical evidence refers to actual things that are collected for review or analysis and provide information to help prove or disprove facts. This includes forensic evidence, like fingerprints, DNA, or toxicology results.

Evidence can also be categorized into direct or circumstantial evidence. Direct evidence directly ties a person to a crime, such as when an eyewitness sees a suspect commit the crime or when fingerprints, recovered from the crime scene, are later identified as belonging to the suspect. Direct evidence produces be clearer link to the suspect than does circumstantial evidence. Circumstantial evidence requires the investigator to draw an inference. For example, a surveillance video shows a suspect going to and/or leaving the area at the time and location at which a crime occurred but does not show the person commit the crime. When circumstantial evidence is used in conjunction with other evidence, it proves to be more conclusive to the jury than when presented alone. A very basic example of the difference between direct and circumstantial evidence can be done with snowfall. If it is snowing in the evening, and then in the morning, there is a fresh coat of snow on the ground, which is direct evidence the snow fell and accumulated overnight. If there was no snow at night and there is snow on the ground in the morning, it can be inferred through this circumstantial evidence that at some point overnight it snowed.

In a criminal investigation in the United States, a jury needs to believe that a crime was committed and that the defendant committed the crime beyond the standard of a reasonable doubt. There are varied legal definitions on reasonable doubt, but their overarching theme is that the jurors do not need to be convinced beyond all doubt. They just need to be convinced beyond a reasonable doubt. This is in contrast with a civil trial where there need only be a preponderance of the evidence. Thus, in civil court, if the side produces 51% of the evidence to support their claim that is enough for a jury to conclude. Criminal trials are held to the higher standard of reasonable doubt for a conviction of a person in trial. The prosecutor bears the burden of proving their case beyond a reasonable doubt, and it is their job to use evidence and witnesses found during the criminal investigation to prove the case to the jury beyond a reasonable doubt. This can be done through a combination of direct and or circumstantial evidence to include witness testimony.

Methods for Gathering Evidence

In this section, the methods for gathering evidence – search warrants, subpoenas, forensic interviewing and interrogation, and technology surveillance – are discussed.

Search Warrants

US society is a democracy based on constitutional rights that value the privacy of the individual (fourth amendment) by preventing a government agent in the investigation of a crime from searching areas that are not open to the public, in

plain view from a public area, or where a person has a reasonable expectation of privacy (Nemeth 2018). This right includes freedom from search in various private locations, such as a person's home, car, technology possessions (phone, laptop, or computers), as well as personal and business bank accounts and records. A law enforcement agent may during the course of an investigation seek the approval of a judge in order to search these areas or obtain private account information through a search warrant if there is probable cause to believe the person committed a crime, search of these locations will result in evidence of the crime, and possessions were used in conjunction to the crime or are pertinent to it (Nemeth 2018). Thus, a judge after reading the warrant and being satisfied that probable cause was appropriately articulated will then sign it. Search warrants are good for specific amounts of time, which vary by jurisdiction, in which the warrant must be executed (Nemeth 2018). In some areas an officer has only 48 h to begin the search, whereas other legislatures allow multiple days before the search warrant needs to be executed or it will expire. A search warrant might be common in a sex assault investigation in which the investigator has probable cause that there is evidence to support the crime in the suspect's residence (Nemeth 2018). The investigator can apply for a search warrant to enter, search for, and seize the evidence as specified in the warrant. Both the locations where they are allowed to search (e.g., suspect's bedroom) and the items they are seeking (e.g., victim's underwear, washcloth used to clean off sperm from victim, used condom) must be specified (Shapiro and Maras 2016). Search warrants can also be used for electronic or online information, such as social media accounts or Internet communication.

Another way information can be obtained is through a subpoena signed by a judge. In this system a judge would sign an order that documents need to be presented to an attorney with an interest in this matter. This can be done by defense and prosecution attorneys and generally is done for trial purposes. In this, most often, it can only be done after criminal charges are filed against an individual. They can require that documents be presented prior to or at the time of trial. Subpoenas requiring documents brought to the trial are often referred to as a duces tecum subpoena. This is in contrast with most subpoenas, which require a person appear in court to provide oral testimony.

Forensic Evidence

After the investigator gets consent from the property owner or a search warrant, then forensic evidence can be gathered. Forensic evidence refers to physical evidence that is collected at the scene or from items at the scene that can, through science, prove or disprove a fact in contention. This physical evidence links the suspect to the crime through contact with the victim, the scene itself, or both. This is often referred to as the *Evidence Linkage Triangle*. The three points of this triangle are the suspect, the victim, and the crime scene, and it is called this term because evidence links these three together. Forensic evidence can also prove elements of a crime. For example, the crime of rape requires penetration. If it is a rape case where penile-vaginal penetration was accused, then a used condom with the suspect's semen on the inside and the victim's DNA on the outside would prove that there was penetration.

Clearly the most probative evidence can specifically identify the perpetrator, but it can both include and exclude in regard to the suspect pool. As Fisher (2004) explained, physical evidence can establish that a crime has been committed or key elements of the crime place the suspect in contact with the victim, scene, or both, establish the identity of associated persons, exonerate the innocent, corroborate the victim's account, and help convince a suspect to confess, and it may be more reliable than an eyewitness. These tasks can be done a variety of ways and through a number of forensic disciplines. For example, fingerprints and footwear impressions provide information about the perpetrator and can help investigators to increase or decrease the suspect list (e.g., eliminate suspects whose prints do not match). Forensic evidence can also link crimes together, which can be very beneficial to an investigator (Nemeth 2018). A serial rapist can leave his DNA at multiple scenes, allowing the

investigator to link rapes from different areas, even if that individual is unknown.

Potentially, the more forensic information gathered at the crime scene, the higher the likelihood that the investigator will be able to use the information to understand known or presumed facts and circumstances of the different cases. The other benefit to forensic evidence is that it can prove facts in contention. Many times, in an investigation, circumstantial information leads to inferences, deductions, and suspicions. Physical evidence, such as a suspect's fingerprints found on an item or in a building, allows the investigator to know the person was in that location or touched that item. This does not solely prove guilt but helps to build evidence in proving it. Other scientific evidence includes bloodstain pattern analysis based on physics and trigonometry (Bevell and Garner 2008). This discipline is defined by subject matter expert Craig Moore as the study of the size, shape, and location of bloodstains in order to determine the physical events which gave rise to their origin. It can provide reliable insight into context and the sequencing of events. Furthermore, it can quickly support or refute claims by involved persons as to what occurred. Forensic evidence can also prove elements of a crime. Rape requires penetration, however slight, as an element of the criminal statute (Nemeth 2018; Shapiro and Maras 2016). If a suspect's spermatozoa are recovered from the vaginal cavity of his victim, then it proves that penetration occurred.

Interview and Interrogation

The purpose of obtaining the subpoena is to compel witnesses to testify in court and to bring documents that are needed as evidence (e.g., phone records) in support the facts of the case (Nemeth 2018). Investigators use interviews to obtain a variety of information from witnesses and victims but rely on interrogations to gain confessions from suspects. Both interviews and interrogations should follow specific guidelines in asking questions, be videotaped, and supplemented by polygraph examination and written statement analyses (Shapiro and Maras 2016).

The evidence obtained through interviewing includes knowledge about the crime itself, identification of a suspect, or even ancillary information about a person, business, or practices leading to the crime. Other information obtained includes insights regarding how the crime was committed, why a person or entity was targeted, and potential motives (Shapiro and Maras 2016). Interviewing can be with a witness, family and friends of a person central to the crime, or with suspects themselves (Shapiro and Maras 2016). If a crime, such as a theft from a business, has a wide array of potential suspects, interviewing can help to narrow the suspect pool and assist the investigator in developing evidence to confirm the correct suspect(s).

Interrogation is similar to an interview, except that the questions are posed to the suspect and focused on the criminal. An interrogation allows an investigator to confront a suspect with the evidence but also allows the suspect to refute this evidence or to explain facts and circumstances around the crime (e.g., mitigating circumstances that may reduce culpability). For example, a driver may have hit and killed a person while speeding but was racing to the hospital with a bleeding child. An interrogation can allow a suspect to confess, that is, to admit guilt and explain the rationale for the crime. Confession is the strongest evidence for an investigator to present in support that the suspect performed the crime. With property crimes, often the perpetrator has a drug addiction and is committing the crimes in order to fuel his or her drug habit.

Technology

Technology is ubiquitous today and offers a number of tools to the investigator. For example, open-source information from the Internet, including social media accounts, can give an investigator great insight into a person's habits, family life, and circle of friends. Another benefit is to reveal information about where a person lives and travels and what is the most important to him or her. A search of telephones, computers, cloud, and other account information to include emails and messaging systems can be highly beneficial to the investigator. Smartphones can be a treasure trove of information, such as location, communication, and photographs that provide time and location,

which could place a suspect at a crime scene, people who served as accomplices, and other sources that could be evidence. This information can help in numerous ways. For example, if conducting a murder investigation, an investigator can determine friends' acquaintances and ways in which the victim spent time from social media in order to determine a suspect pool or perhaps a motive. A person may post information about items for sale that the investigator knows to be stolen. Or, in a sexual assault, a person may send a message or have a dialogue on social media in which admit actual acts or at least place themselves in the area at the time of the incident being investigated. Forensic experts are able to record and use an electronic crime scene with digital and electronic evidence. The rapid technological advancements through the digitalization of data and information is difficult to detect and fragile and requires specifically skilled investigators who keep up with the changes in the field (James et al. 2014).

Another technology tool is the surveillance camera, used both inside and outside businesses as a means to prevent crime but also to help locate perpetrators and provide evidence in criminal prosecution (Nemeth 2018). Most municipalities have cameras to help cover public areas like roadways, parks, and government buildings. Nearly every individual in the United States has a smartphone that would allow the person to record any activity of interest instantaneously. Investigators must use this opportunity to obtain evidence for the cases they are investigating to provide what exactly occurred, who was there, and who committed the offenses. Cameras can show people and vehicles in an area, either before, during, or after an offense – simultaneously capable of providing evidence that a suspect was the culprit but also exonerating a suspect (i.e., prove an alibi).

Image analysis recognition and evaluation are becoming important technology tools to support these investigations by analyzing or enhancing surveillance or other videos (James et al. 2014). These tasks use the familiar Adobe Photoshop (need R) to sophisticated specialized software. This is an ever-developing area of technology with the increase in surveillance video. Face recognition technology is one of these developing areas and is becoming used both in the review of video, as well as in live feeds. Many areas of the country are installing LPR or license plate reading cameras in high-traffic areas to capture license plates and enable law enforcement to identify vehicles used in crimes quickly. Allegheny County District Attorney Steven A. Zappala, Jr. is a leading law enforcement proponent of this technology, and his office has spearheaded and provided funding for LPR cameras not only throughout Allegheny County but also in high-traffic areas of adjoining counties. D.A. Zappala is also advocating to use it to create virtual checkpoints at schools and other areas that may be targets as part of a safeguarding effort. The project currently includes nearly 300 cameras over all with 30% containing LPR technology.

If an investigation includes ongoing activity, such as a string of thefts or even a robbery from a safe, then cameras can be used to surveil the area and to catch the perpetrator committing the crime itself. Microphones can be used to record audio and conversations. The legality of using this technology depends on local laws regarding the use of recording devices, specifically audio recordings. States vary regarding the recording of conversations. In some states it is a felony to surreptitiously record any conversation. Even police cannot record conversations without consent of both parties or an order from a judge. Other states (e.g., NY) allow recording conversation if one party consents, even if the other person is not aware it is being recorded. Investigators need to exercise caution and be familiar with laws anytime they consider employing a recording device as part of an investigation. In the next section, the two types of crime investigations (persons, property) are described.

Crimes Against Persons Investigations

Death Investigations

The most serious crime in society is the taking of a life, so death investigations are paramount when it comes to prosecuting suspects with this criminal violation. A death investigation is multifaceted

and can drain resources, depending on the complexity of the investigation (Nemeth 2018). Hess et al. (2017) outlined important steps an investigator should take in a death investigation. These include assigning multiple detectives, detailed notes at the crime scene, following up on all leads, interviewing all potential witnesses, and attending the autopsy. One of the early steps is an examination of the body, as well as the scene surrounding it. The examination of the body begins with observations noted by detectives or crime scene personnel processing the scene. Here the body is visually examined to make a number of determinations, specifically: (a) estimating an approximate time of death, (b) determining whether the body has been moved, and (c) determining whether there are signs of trauma on any areas of the body.

A time of death is important as it allows the investigators to set a time frame in which to consider likelihood of alibis by various suspects, confirm probability or rule out suspects, and determine which potential witnesses to interview. Witnesses or known persons to the decedent are most likely to help in this process of setting the parameter for time of death estimation, particularly last known time alive, when first discovered, and other elements surrounding the time frame. The rough timetables from these witnesses, as well as other factors such as the temperature of the body, can help to form a rough notion of the time of death, which increases in accuracy when discovery is shortly after death.

If the body has been moved, it is "red flag" suggesting it could be a homicidal death. While there are reasons a body is moved for lawful purposes – such as EMT – first responders rendered first aid/CPR, or police first responders searched for identification. There are a number of things that can help determine if a body has been moved. One such thing is lividity, which is the settling of the blood. In this process, after death, the blood settles by gravity settles to the lowest point. It then becomes fixed in this position on a somewhat consistent timetable. If the lividity is not consistent with the manner in which the body was found, then investigators can extrapolate that the body was moved after the lividity became fixed, that is, postmortem. Rigor mortis is the stiffening of the muscles after death. This also exhibits and then later fades at a somewhat consistent time frame. However, it can be affected by a number of factors too, such as the decedent having a fever prior to death or strenuous activity preceding death. Those factors need to be weighed, but rigor can also alert investigators if a body has been moved prior to rigor mortis setting.

Trauma to the body may be paramount to the investigator determining whether the death was accidental or homicide (Nemeth 2018). It can indicate how the decedent died, as well as circumstances surrounding the events which led to a person's death, and the mechanism that likely caused the death, such as gunshot wounds, stab wounds, blunt force trauma, and something as small as a needle puncture mark in a drug overdose death. After discovery, the body will be taken to a facility, such as a Medical Examiner's Office where an autopsy can be performed by a forensic pathologist. A forensic pathologist is a medical doctor who has continued their training into pathology and later forensic pathology so that they can specialize in determining causes of death with specific training as to injury and other mechanisms of death. It is important to remember that while an investigator at the scene can make observations about injury, the final conclusion is made by the forensic pathologist who is the paramount expert.

Sex Assault Investigations

A sex assault investigation is an umbrella term that incorporates a number of sexual crimes, (e.g., rape), involuntary deviant behavior, domestic violence (e.g., elder abuse, child sexual abuse), and unwanted touching (Nemeth 2018; Shapiro and Maras 2016). These crimes, like death investigations, are multifaceted, and the investigation of the scene is important for collecting forensic evidence. It is important to remember that with the exchange of bodily fluids in a sex assault case, clothing, objects, towels, napkins, used condoms, and the victim's body may all contain forensic evidence (Nemeth 2018; Shapiro and Maras 2016). Child victims should be seen in a child

advocacy center (i.e., a trauma unit with specially trained medical staff), whereas adult victims need to be seen at a hospital that has trained sex assault nurse examiners (SANE) to ensure that potential evidence in or on their bodies is collected (Nemeth 2018; Shapiro and Maras 2016).

A sexual assault is arguably the most devastating experience a person can endure. The investigation is difficult largely because of the psychological damage perpetrated upon the victim, and the stigma of sexual crimes results in shame and guilt feelings by the victim (Shapiro and Maras 2016). As an investigator, it is a difficult and sensitive task to collect the evidence, interview the victim, and prepare for prosecution while preserving the integrity of one's case and the dignity of the victim (Nemeth 2018; Shapiro and Maras 2016). In sexually based crimes, the perpetrator may be a health professional, stranger, friend, acquaintance, spouse, family member, or intimate partner. An investigator must extract every painful detail from the victim in order to proceed effectively, and the victim may later be called upon to repeat this process in court (Nemeth 2018; Shapiro and Maras 2016).

The relationship to the perpetrator is important to establish, and in the vast majority of cases, the victim knows the perpetrator and identifies the person as an intimate partner, friend, or acquaintance (Shapiro and Maras 2016). In these investigations the focus shifts its focus to the collection of evidence that establishes the absence of consent for adults (minors by definition cannot provide legal consent) and/or the presence of force or threat because this tactic may be necessary to counter the perpetrator's defense that the "victim" consented (Minnesota Center Against Violence and Abuse 1998–2005). Investigators should make sure that they are not harboring animosity toward the suspect that may erroneously result in a confirmation bias (i.e., look for evidence of guilt while ignoring exculpatory evidence). The crime of sexual assault, particularly against minors, is considered to be particularly heinous by the public, so investigators should ideally be reasonably sure of the suspect's guilt prior to accusations or the commencement of a criminal prosecution. The consequences of bias are that the investigator is professionally and/or personally ruined from even an allegation if it proves to be false.

There are limitations to investigative capabilities that may hinder evidence gathering. For example, an accused person has no requirement legally to speak with the investigator or even the police, leaving only the victim's testimony as the only evidence (Nemeth 2018; Shapiro and Maras 2016). Additionally, children are not seen as reliable witnesses prior to ages 12–14 years, so often the prosecutor will not proceed unless there is a confession (Shapiro and Maras 2016). Finally, it is unclear whether the sexual assault incident rates are accurate given the self-report research suggesting that many rape incidents go unreported (Shapiro and Maras 2016). The rates of reported and unreported sexual assaults vary due a several factors, such as how the crime is defined, what population is studied, and what methodology is used.

Crimes Against Property Investigations

Crimes against property typically include theft, robbery, and burglary. Theft or stealing is delineated from robbery in that the latter uses force or a threat of force on the victim (Nemeth 2018). If someone steals an item from a store such as in shoplifting, it is a theft. However, if they threaten or assault the clerk in the process (e.g., brandishing a weapon, such as a gun or knife) while demanding money, then it is a robbery (Nemeth 2018). Even if the gun is not real, it is a robbery as there was a threat of force in the eyes of the victim. Robberies and thefts tend to happen quickly, and often there is not much forensic evidence unless a weapon is used, items are touched, or clothing or other items are discarded or dropped during or while fleeing the crime.

A burglary involves entering a building or occupied structure (residential or commercial) for the purpose of commit a crime therein (Nemeth 2018). It is most commonly associated with entering a commercial establishment when is closed or residence and stealing valuables from inside. The underlying crime here is a theft of

property, but it is a burglary because they entered the structure to commit this crime. It is a common myth that residential burglaries most often happen at night while people are sleeping. This is not true, and most burglars only want your valuable and do not want to be confronted or be in a situation of possible violence. Most often, burglars break into businesses at night when they are closed and residences during the day when the occupants are away at work or school. Hess et al. (2017) indicated that burglary has a national average of a 13% clearance rate. This is partially due to it being a common crime, as well as being a crime lacking strong ties between the perpetrator and the victim, resulting in a large suspect pool. This commonality and low clearance rate reinforce the need for a quality preliminary investigation (Hess et al. 2017).

Physical evidence in crimes against property include the items used for the commission of the crime, the stolen property, and biological forensic evidence (e.g., fingerprints, blood, hair, skin). For example, sometimes in burglaries and robberies, the assailants injure themselves and leave their blood at the crime scene. Most property cases are investigated through interviews of the victim and witnesses, interrogations of suspects, and, when possible, surveillance video. In burglaries, thefts, and robberies, an investigator can also attempt to follow the property and locate it if it is sold or offered for sale. This can be tracked through Internet sales or pawnshops. It is easier to track and locate rare, valuable, or otherwise individualized items. For example, a class ring or a watch with an inscription is easier to track than diamond stud earrings that are common and often unremarkable.

Crimes Against Society

Fraud cases often leave a paper or electronic trail. These often use interstate communication devices such as phones, computers, the mail system, or financial and banking institutions (Hess et al. 2017). A specialist such as a forensic accountant may be needed if it was a complex crime such as an embezzlement especially if it occurred over a number of years. In these cases, finding a paper or electronic trail is key to the investigation. The old adage of "follow the money" rings especially true here and can generally point to the person or people perpetrating these crimes. Often this can involve multiple people in key positions where they have access to funds or the ability to cover the trail of the person perpetrating the crime. This may need searches of not just the business accounts but warrant that allow an investigator to access the information for a suspect's private account. In cases where a specific person has been defrauded by another, the "fraud victims are in a good position to provide information regarding the suspects because they had first-hand dealing with the suspects" (Hess et al. 2017).

Conclusion

There are untold number of investigations a year that occur from law enforcement and private security professionals through the United States and the world. These investigations vary from minor offenses of traffic infractions and low-level threat to the most heinous of criminal activity such as rape and murder. It is imperative for these investigations to act quickly but cautiously. Beginning these investigations without delay gives the greatest chance for being able to locate the largest amount of evidence. This includes collecting surveillance videos that will overwrite itself over time, biological evidence like DNA that will degrade or be washed away, as well as evidence that can be intentionally destroyed by a suspect or a party interested in the defense of the suspect. Also, identifying and interviewing those that may have been a witness or have information about the activity should be completed sooner than later. An investigator needs to be cautious that they are examining the evidence from an unbiased perspective that they consider all of the facts and possibilities while they narrow what is possible and who is likely responsible for the illegal acts. The caution also is important in being sure that an investigator does not violate the law in their

pursuit to recover evidence. A government law enforcement official needs to know when they need consent or a search warrant prior to gaining access to an area or item to search for and potentially collect evidence. In the end all of the items and factors need to be weighed in order to draw inferences and determinations in regard to what occurred, if it was a criminal act, and who or whom perpetrated these crimes.

Cross-References

- ▶ Interviewing Adults: Communication at the Front Line
- ▶ Interviewing Children
- ▶ Investigations: Burglary
- ▶ Investigations: Polygraph Use
- ▶ Investigations: Sexual Assault
- ▶ Investigations: Use of DNA and Fingerprints

References

Bevell, T., & Garner, R. M. (2008). *Bloodstain pattern analysis: With an introduction to crime scene reconstruction* (3rd ed.). Boca Raton, FL: CRC Press.

Burgess, A. W., Roberts, A. R., & Regehr, C. (2009). *Victimology: Theories and Applications*, Jones & Bartlett Learning, p. 103

Fisher, B. A. (2004). *Techniques of crime scene investigation*. Boca Raton, FL: CRC Press.

Hazelwood, R. R., & Burgess, A. W. (2009). *Practical aspects of rape investigation: A multidisciplinary approach* (4th ed.). Boca Raton, FL: Taylor & Francis Group.

Hess, K. M., Orthmann, C. H., & Cho, H. L. (2017). *Criminal investigation* (11th ed.). Boston: Cengage Learning.

James, S. H., Nordby, J. J., & Bell, S. (2014). *Forensic science: An introduction to scientific and investigative techniques* (4th ed.). Boca Raton, FL: Taylor & Francis Group.

Minnesota Center Against Violence and Abuse. (1998–2005). Successfully investigating acquaintance sexual assault: A national training manual for law enforcement. Accessed at: http://www.endvawnow.org/uploads/browser/files/Successfully%20Investigating%20Acquaintance%20Sexual%20Assault%20-%20A%20Natl%20Training%20Manl%20Law%20Enforcmt.pdf

Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton, FL: CRC Press.

Shapiro, L. R., & Maras, M.-H. (2016). *Multidisciplinary investigation of child maltreatment*. Burlington, MA: Jones & Bartlett Learning.

Woods, D. D., Jr. (2013). *O'Hara's fundamentals of criminal investigation* (8th ed.). Springfiled, IL: Charles C. Thomas.

Further Reading

Bell, W. R. (2002). *Practical criminal investigations in correctional facilities*. Boca Raton, FL: CRC Press.

Gardner, R. M., & Krouskup, D. (2019). *Practice crime scene processing and investigation* (3rd ed.). Boca Raton, FL: CRC Press.

Geberth, V. J. (2010). *Sex-related homicide and death investigation: Practical and clinical perspectives* (2nd ed.). Boca Raton, FL: CRC Press.

Geberth, V. J. (2014). *Practical homicide investigation checklist and field guide* (2nd ed.). Boca Raton, FL: CRC Press.

Investigations: Cybercrimes

Michelle D. Miranda
Farmingdale State College, The State University of New York, Farmingdale, NY, USA

Keywords

Cybercrime · Investigation · Digital · Forensics · Crime scene

Definition

Cybercrime investigation: An investigation focused on crimes in which digital technologies were used in the commission of the criminal act.

Digital forensics: A branch of forensic science focused on the scientific analysis of digital devices and their application to matters of legal significance.

Investigation: To observe and study utilizing scientific inquiry, reasoning, and analytical methodologies with the goal of gaining knowledge and understanding about individuals and/or events.

Introduction

Cybercrime is broadly defined as the use of digital technologies in the commission of a crime. These digital technologies may include hardware (computers and peripherals, mobile phones, cameras, storage devices such as thumb drives and hard drives, office equipment such as copiers or scanners, servers, digital home assistants, smart appliances, personal wearable devices, gaming consoles, drones, and myriad devices with a digital component) and software as well as the Internet and related cyberspace (e.g., social media, cloud services, and data transmitted via the Internet of Things). From a forensic perspective, approaching cybercrimes requires consideration of investigative matters; procedural elements including the prosecution and defense of cybercriminals and any related legal matters, such as evidence admissibility and (electronic) discovery; and legislative oversight, which encompasses the legal system's responses to cybercrimes and includes statutes that guide cybercrime investigations and prosecutions (e.g., dealing with matters pertaining to searches and seizures).

Cybercrime investigations include the identification, acquisition, recovery, and safeguarding of electronic traces, as well as any analysis and interpretation of digital data. Data is material which serves as apparent facts as applied to the investigation; raw data may be subject to authentication, analysis, and interpretation and further structured in a systematic manner during the course of an investigation. Cybercrime investigations are guided by several factors, including: the nature or type of crime (e.g., DDoS attacks, child pornography, human trafficking, identity theft, electronic espionage, or cyberterrorism); the type of digital technology recovered or data contained and extracted therein; and the scope of the crime (public/criminal, private [corporate]/civil, transnational/international). Digital traces in a cybercrime investigation are sought to: establish that a crime has been committed; provide location data to support or refute witness statements; develop a timeline of events; or aid in developing patterns in user activity to link criminal behavior. A trace is the remnant of an action, individual, or object in a location or space, and must be decoded and understood to elicit some knowledge about the event (see Margot 2011, p. 91, 2017, p. 32). The examination and interpretation of digital data must be considered in context, and as such, cybercrime investigations incorporate information obtained during the course of the broader investigation, including the recognition and interpretation of physical traces (e.g., fingerprints and DNA), information obtained during witness interviews, and any matters related to standard forensic and police investigation methods into the overall reconstruction of events.

This entry considers three critical components of cybercrime investigations, specifically the physical (or crime scene) investigation, the digital (or laboratory) investigation, and the investigator. Each type of cybercrime will have its own specific investigative approach with respect to procedure and analytical methodology, as will the type of digital technology encountered, but there are general guidelines for cybercrime investigations that establish the foundation of such endeavors. Finally, this entry briefly considers the growing area of scholarship in criminological and psychological approaches to understanding cybercrime.

The Cybercrime and Digital Forensic Investigator

The cybercrime investigator requires general criminal investigation skills as well as specialized knowledge and experience with digital technologies such that the investigator can apply their expertise to a digital, or virtual, environment. The investigator should have formal knowledge and experience in the following:

1. Methods of detection and investigation ("police science"), including interviewing and interrogation. The investigator should be versed in administering investigative interviewing techniques such as the cognitive interview and should be familiar with deception detection.

2. Intelligence analysis. The digital investigator should be able to take their observations and raw digital data ("information") collected during the initial phases of an investigation and be able to extract and interpret the most relevant data to produce a meaningful assessment and interpretation ("intelligence").
3. Analytical reasoning skills. The investigator should be able to begin their scientific methodology by asking the right questions in order to define the scope of their investigation. This method should include the utilization of abductive, inductive, and deductive reasoning to form meaningful hypotheses and adapt lines of inquiry as they progress through their analysis. Investigators should be able to identify relationships and patterns in the data and should be aware of cognitive biases or analytical variation that may warrant control measures or calculations of error.
4. Technical and scientific knowledge about digital traces and the interrelationship between digital and physical traces. The investigator should be able to recognize and handle digital traces and related devices so as to minimize loss and damage while maintaining the integrity of the digital media. Recognition and handling of traces are critical aspects of an investigation and may often be the most important factors in a case. In addition to the general volatility of digital traces, handling digital traces may vary depending on the status of the device at the time it is first encountered. The investigator should have knowledge of peripheral and associated devices when collecting digital technology, whether it be a media card or a power cord. Furthermore, the investigator should also have knowledge about whether or not a device requires an uninterrupted or continuous source of power. For example, the handling and packaging of a mobile device requires consideration of whether it is discovered on or off, whether it is locked or unlocked, whether or not it is actively connected to a network, and whether or not it exhibits signs of attempted destruction or damage (e.g., smashed or submerged in a liquid). The investigator should be aware of the nature of any digital and electronic media, including the location of unique identifiers (serial numbers), how to repair a device in the event that there is physical damage, and general information regarding default or standard operating systems for a given device. Knowledge of anti-forensics has also become a critical aspect of digital investigations and must be part of the digital investigators skill set. Finally, the investigator should be aware of the potential for physical traces such as fingerprints or biological traces (e.g., a blood or saliva stain that may be submitted for DNA analysis). Awareness of such traces should include the ability to acknowledge the potential for such traces to be present on a digital device as well as the ability to properly secure, package, and store the digital device to preserve and maintain the integrity of both the digital and physical traces for further analysis;
5. Legal and procedural requirements (for domestic and international investigations and prosecutions), both general and specific to digital evidence. Such knowledge includes matters pertaining to privacy; search and seizure; rules of evidence (admissibility); internal policies and procedures such as those that may be in place within corporations and government agencies; policies and contracts such as those that may be administered by third-party service providers; challenges to international investigations (including technical matters such as criminal enterprise, sophistication and technology; jurisdictional matters such as state sovereignty; and legal matters such as agreements, procedural requirements for requesting legal assistance, evidence acquisition, extradition policies, and any limitations to existing practices).

With respect to stored electronic communications and general content data, Brown (2015) provides a useful overview of service providers and avenues of inquiry for investigations (69). Brown further weighs in on the "human side of a cybercrime inquiry which is pivotal for giving meaning and weighing significance" to digital traces, providing a list of desired skills and related competencies of an investigator (2015, p. 64). These

include experience and what Brown divided into general, "soft" digital forensics investigative skills and technical, "hard" digital forensics investigative skills (2015, pp. 65–66). Brown's soft investigative skills include communication, collaboration, and rationality, while the hard investigative skills include structured, unstructured, and semi-structured data analysis, reverse engineering, programming and scripting, and virtualization. INTERPOL (2019) also developed a "non-exhaustive skillset checklist," which lists data recovery, computer forensics, mobile phone forensics, network forensics, audio, video, and image forensics, and emerging technologies forensics (e.g., Internet of Things forensics) as necessary analytical skills (58–59).

Physical [Crime Scene] Investigation

Crime scene investigation contributes to the fact-finding objective of an investigation and does so by aiding in identification and reconstruction. Described by De Forest (2005) as a recording medium, the crime scene can aid in establishing links between the event, the perpetrator, and the victim by way of physical and digital traces left behind. Digital traces may include documents and records, photographs and digital images, audio and video recordings, and geolocation data, as well as digital devices that may serve as secondary crime scenes containing additional digital traces in a virtual environment. It is important here to distinguish crime scene processing and crime scene investigation. The former, crime scene processing, is a "bag and tag" operation to be conducted by a technician, while the latter, crime scene investigation, is a scientific endeavor of recognizing traces, whether physical or digital, and applying the scientific methodology and analytical reasoning that will lead to a meaningful reconstruction that can further contribute to the cybercrime investigation. De Forest (2005) highlights the need for educated, experienced scientists at the crime scene, and this idea can be extended to the need for individuals with added digital expertise at crime scenes dealing with cybercrimes and digital forensic investigations.

Crime scene investigation is characterized by utilization of a scientific and methodical approach, which includes observation, analytical reasoning, and iterations of developing and modifying hypotheses as new observations are made and data is acquired, whether the data results from laboratory analysis of the physical and digital traces or from "traditional" investigatory methods including witness statements during investigative interviewing. Investigators should be aware of cognitive biases and fallacies in their reasoning and account for such in their investigative process.

Recognition and identification of digital traces is not isolated to the immediate crime scene but also includes assessing the scene and its surroundings for CCTV footage, digital images from mobile devices, social media posts, and access control technologies. Investigations may also include evaluating historical and archived digital media in the form of records, images, and videos. In addition, investigations may include thorough observation, examination, and analysis of a scene for comparison to earlier video footage, photographic materials, audio recordings, or geolocation data at the same location in an effort to establish links and reconstruct a plausible sequence of events.

The act of "processing" the physical crime scene involves collecting, packaging, transporting, storing, and documenting traces identified within the scene. Collection and packaging require consideration of the nature of the evidence, including the presence of adhering physical traces. Care must be taken to prevent loss or destruction of digital and physical traces during handling and packaging. Specialized packaging may be necessary for digital devices and may include the utilization of Faraday bags, anti-static bags, or any alternate electromagnetic radiation-blocking containers. Documentation should be contiguous and detailed, and should include notes and photographs. Records should be kept to maintain chain of custody and unique identifiers should be utilized for each item recovered.

It may be necessary to evaluate digital devices at the scene and determine whether or not they should be recovered for analysis in the laboratory or whether they should be examined in the field

for purposes of extracting data. Such field examinations may be conducted in an effort to save time or reduce the number of items submitted to the laboratory, especially in those circumstances where there is a large amount of digital data known to be of no significance to the investigation, or in cases where there are minimal resources allocated for digital investigations within the laboratory (e.g., lack of trained analysts/investigators and equipment). With respect to determining the feasibility of onsite versus offsite searches, Maras (2015) notes the following factors: the configuration of the hardware or software, the overall size and complexity of the system, and the technical demands of the search (35). In general, investigators responding to the scene should at least be able to properly process the devices (collection, packaging, transport, storage, and documentation as described above) to prevent loss or damage and ensure the integrity of the items recovered and the traces therein. When in doubt, data extraction or recovery should not be attempted by inexperienced individuals at the scene and should instead be conducted in the laboratory by experienced digital analysts/investigators.

Digital [Laboratory] Investigation

Laboratory analysis of digital traces during a cybercrime investigation should be marked by analytical integrity by way of chain of custody and record maintenance, standard operating procedures, and functional autonomy through quality assurance and method/tool/instrument validation. Procedures should be developed such that they are scientifically robust (e.g., transparent and reproducible) and allow for analyst/investigator flexibility should their findings result in alternate lines of inquiry. According to the International Organization for Standardization (ISO), "The incident under investigation should be clearly identified and defined, including limitations to the scope of the investigation. Sources of potential digital [traces] and questions to be answered should be identified. Sources of risk and their potential effects on the investigation, personnel, and systems should also be identified" (ISO/IEC 27041: 2015a, p. 6).

Various investigation process models have been developed as a means of providing a step-by-step approach to digital investigations since the first digital forensics research conference approached the topic in 2001. One result of the conference was the development of a process model for digital forensic investigations, which was included in a technical report entitled *A Road Map for Digital Forensic Research*. Workshop attendees produced a linear process consisting of Identification→ Preservation→ Collection→ Examination→ Analysis→ Presentation→ Decision (Palmer 2001, p. 17). There have been myriad proposed models since 2001, which are largely assessments and reiterations of the same core steps (planning/preparation; scene processing; data acquisition/analysis; reporting/presentation). In 2008, Carroll et al. (2008) developed a *Digital Forensic Analysis Methodology* flowchart in an effort to contribute to the early development of a digital investigative method. This flowchart highlights three major parts of the process: preparation/extraction, identification, and analysis. In their flowchart, Carrol et al. pose a series of specific "Who, What, Where, When, How and Other" questions to guide the investigator during the analysis phase. In the same year, Marcella and Menendez (2008) presented "a structured approach to cyber forensic investigations" with a *Flowchart for the seizure of electronic evidence and associated internal control questions* (193).

After numerous process model iterations, ISO released in 2015 a "harmonized digital investigation model" in the form of a flowchart depicting a series of processes and associated subprocesses (ISO/IEC 27043: 2015b, p. vi). The primary processes include readiness, initialization, acquisitive, investigative, and concurrent, with the acquisitive and investigative stages consisting of the bulk of the analytical portions of a digital investigation. The acquisitive process deals with the physical (crime scene) investigation of a case in which digital traces are identified, collected, and acquired. The identification and collection subprocesses as

presented would be equivalent to the identification/recognition and processing discussed above. The acquisition subprocess within the acquisitive stage is described as "optional," for the reasons noted above regarding evaluating onsite versus offsite data acquisition. The investigative process deals with the acquisition, examination, analysis, and interpretation of digital traces. With respect to interpretation, the document asserts, "One goal of the digital evidence interpretation process is to use scientifically proven methods to construct explanations for the presence of the digital artefacts identified. . .within the context of the investigation. If the contextual information changes, the interpretation may also have to change in order to reflect" such changes (ISO/IEC 27041: 2015a, p. 19). More recently, INTERPOL (2019) presented a series of flowcharts addressing the acquisition process, computer examinations, and a process of analyzing [an] exhibit's artifacts (68–70).

Proceeding with analysis requires knowledge about the nature (type) of the recovered media and consideration of the data to be recovered. Such considerations may include accessibility: direct access (to data such as documents, photos, videos, emails, internet browser history, specialized software, programs or applications, social media, peer-to-peer files, log files, stored data), remote access/analysis, and stored v. real-time data (subscriber data, traffic data, and content data; see UNODC 2013, p. 123). After making such assessments, the analyst/investigator can move forward with selection of the analytical tool that should be employed. Selection and utilization of specific tools is critical for guiding decision-making and hypothesis testing, including the selection and order of subsequent analytical procedures. Considerations should include specification, performance capabilities, reliability, search or analytical parameters, and limitations (potential for errors). The latter consideration requires the analyst/investigator is knowledgeable about detecting and troubleshooting such errors and inconsistencies (manual intervention), conducting risk assessments, and reporting any error estimates or statistically significant deviations. In general, the tools employed and the analytical methods used should be validated and documented: "Before using a preferred tool or method to conduct an investigation the investigators should consider the likely effects of all the weaknesses of the complete process sequence selected. A formal understanding of the weakness of a process enables theses errors to be effectively controlled through the use of correct process selection and robust documented risk analysis or assessments" (ISO/IEC 27041: 2015a, p. 8).

The acquisition, or retrieval, stage of a digital investigation is often akin to a secondary crime scene investigation and must consider the elements of digital trace recognition and collection. Acquisition may be direct or remote. Direct acquisition is marked by drive imaging and content duplication (copying) and recovery of data, which requires consideration of operating systems and configurations, the amount of data, and whether there will be dead (no power) v. live (actively running) system acquisition (see INTERPOL 2019, p. 32). For dead systems, INTERPOL advises considering the following: active files, deleted files, file slack, partition slack, disk slack, and shadow files; device artifacts, operating system files, file registry, file metadata, encrypted files, log files, and database files; browsing history, e-mail, social media, and peer-to-peer file sharing (INTERPOL 2019, p. 41). For live systems, INTERPOL advises considering the following: random access memory, running processes, network connections, system settings, storage media, and cloud storage (INTERPOL 2019, p. 42). Further considerations include locating deleted, hidden, encrypted, password protected, or otherwise concealed or manipulated data (steganography, cryptography). Additional analytical steps include searching, sorting and filtering data, which involves identifying space (slack, unallocated) and partitions; and the recovery or extraction of data. INTERPOL further describes logical extraction (accessible storage media) and manual extraction (inaccessible storage media as a result of electronic or mechanical failure) of data as well as data isolation techniques (manual methods, wireless jamming, Faraday shielding; see INTERPOL 2019, p. 35, 37).

"The opportunity for recovery of digital [traces] will depend on many factors, including

the volatility of the original data to be acquired, the age and condition of the item submitted, automatic system deletion of unallocated data and the level of security features applied by the original user" (ENFSI 2015, p. 32). Each analytical step requires an element of human assessment and problem-solving on the part of the examiner/investigator. The analytical process may be iterative based on the nature of recovered digital traces. The data recovered is subject to interpretation, in which the investigator will consider the significance of the data and transform the information into intelligence. The data and any interpretations can be applied to a reconstruction of events to determine locations and transmission of information and develop a sequence of actions.

A critical component of data analysis is authentication. It is important to verify data integrity (e.g., by way of identification of digital hash values) and overall continuity of the data, and in many cases, assign attribution, authorship, and ownership to digital devices and the traces therein. The UNODC (2013) notes that, "the party offering the evidence must demonstrate that the digital information obtained from the device is a true and accurate representation of the original data contained on the device ('authenticity') and that the device and data sought to be introduced as evidence is the same as that which was originally discovered and subsequently taken into custody ('integrity')" (158). The investigator should keep in mind that authentication can be supported or refuted by "traditional" investigatory methods and supplemental physical traces.

Network investigations may result as a response to intrusions, attacks, or suspected cyberterrorism. Such investigations require specialized knowledge of network security tools and access control methods in a virtual environment. Network investigations may involve surveillance and monitoring in real time or live time, obtaining traces from an active device or intercepting communications utilizing hardware, a virus, or a keystroke logger. In addition, in cases of high volumes of data, the analyst/investigator must be able to filter data during the analytical process and look for patterns within the data. Network investigations may also involve criminal or geographical profiling techniques to identify perpetrators or locations. As with direct analysis on recovered digital devices, data integrity and the utilization of robust methods are of critical importance.

Criminological and Psychological Considerations

Two areas of cybercrime investigation gaining attention and scholarship are cybercriminology and the psychological assessment (behavioral analysis) of cybercriminals for purposes of offender profiling. Cybercriminology presents a criminological approach to understanding cybercrime, the cybercriminal, and the victim (victimology; cybervictimization). Maras (2017) asserts, "cybercriminology tests the applicability of mainstream criminological theories to cybercrimes committed. . . [and] seeks to shed light on the nature and extent of cybercrime, assess reactions to cybercrime and the implications of these reactions, and evaluate the efficacy of existing methods use in the control, mitigation, and prevention of cybercrime" (13).

Behavioral analysis during the course of a cybercrime investigation can aid in reducing the number of possible suspects, determining the motive behind a cybercriminal's activities, tracking a suspect, identifying associates in a criminal enterprise, and in some instances, identifying the perpetrator(s) of the cybercrime. With respect to the latter, identification can be facilitated by assessment of the type of attack and the target, the skill level of the attacker, and stylistics (see, for example Steel 2014). Forensic stylistics is the examination of style in [written] language including grammar, syntax, spelling, vocabulary, and phraseology for the purpose for resolving questions related to disputed authorship or meaning (Kingston and Stalker 2006, p. 95). Casey (2006) notes, "the basic concept underlying behavioral evidence analysis is simple—offenders leave an imprint of themselves at the crime scene, and their actions and communications tell us something about the individual" (58). Linguistic surveillance can be utilized to aid in the identification of the perpetrator, and can also be useful for threat

assessments to measure perpetrator credibility and seriousness of the crime during a cybercrime investigation.

Conclusion

Taking on digital investigations requires balancing digital knowledge and investigative experience. Goodison et al. (2015) conducted a needs assessment and identified problems on both front end (crime scene) investigations and back end (laboratory) investigations ranging from deficiencies in personnel, funding, tools, and technologies to challenges in accessing and analyzing specific types of devices and data therein. One noted challenge involves first responding officers to an incident or arrest that do not know how to properly recognize or secure digital devices. Proposed solutions include providing general training focused in the identification and processing of digital devices and traces at crime scenes for police academy recruits, training recruits in law and cybercrime, and specific training focused in advanced digital investigations to those individuals in an investigatory (detective) track (see, for example, proposed solutions applied to the recovery and analysis of digital evidence in sexual violence investigations presented by Maras and Miranda 2017). Such training would be similar to the training recruits and detectives receive presently on the subjects of physical traces and DNA. Another noted challenge is that analysts and investigators must maintain current with respect to the recognition, collection, preservation, and analysis of new and evolving digital technologies, as well as the anti-forensics efforts developed to hinder such investigative endeavors. One proposed solution is certification and continuing education for digital forensic investigators. Both the development of programs for effective education and training of digital investigators and the development of standard investigative methods of conducting digital forensic investigations are underway to meet the increasing number and types of cybercrimes encountered in both the public and private sector. Due to the transnational nature of cybercrimes and the increased sophistication of cybercriminals and technologies, the utilization of tools such as behavioral profiling may prove useful for identifying the cybercriminal based on their motivations and methodologies. The application of criminological and psychological approaches to cybercrime can thus enrich cybercrime investigation processes.

Cross-References

- ▶ Criminals: Cybercriminals
- ▶ Investigations: Criminal

References

Brown, C. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55–119.

Carroll, O., Brannon, S., & Song, T. (2008). Computer forensics: Digital forensic analysis methodology. *United States Attorney's Bulletin, 56*(1), 1–9.

Casey, E. (2006). Editorial: The value of behavioral analysis on digital investigation. *Digital Analysis, 3*(2), 57–58.

De Forest, P. (2005). Crime scene investigation. In L. Sullivan (Ed.), *Encyclopedia of law enforcement*. Thousand Oaks: Sage Publications.

European Network of Forensic Science Institutes. (2015). Best practice manual for the forensic examination of digital technology (ENFSI-BPM-FIT-01).

Goodison, S., Davis, R., & Jackson, B. (2015). Digital evidence and the U.S. Criminal Justice System. RAND Corporation, Santa Moncia, CA.

International Organization for Standardization. (2015a). Information technology—Security techniques—Guidance on assuring suitability and adequacy of incident investigative method (ISO Standard No. 27041:2015).

International Organization for Standardization. (2015b). Information technology—Security techniques—Incident investigation principles and processes (ISO Standard No. 27043:2015).

INTERPOL. (2019). Global guidelines for digital forensic laboratories. INTERPOL Global Complex for Innovation.

Kingston, J., & Stalker, K. (2006). Forensic stylistics in an online world. *International Review of Law Computers and Technology, 20*(1&2), 95–103.

Maras, M.-H. (2015). *Computer forensics: Cybercriminals, laws and evidence*. Burlington: Jones & Bartlett Learning.

Maras, M-H. (2017). Cybercriminology. Oxford University Press.

Maras, M.-H., & Miranda, M. D. (2017). Overlooking forensic evidence? A review of the 2014 international protocol on the documentation and investigation of

sexual violence in conflict. *Global Security: Health, Science and Policy, 2*(1), 10–21.
Marcella, A., & Menendez, D. (2008). *Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes* (2nd ed.). Boca Raton: Auerbach Publications.
Margot, P. (2011). Forensic science on trial—What is the law of the land? *Australian Journal of Forensic Sciences, 43*(2–3), 89–103.
Margot, P. (2017). Traceology, the bedrock of forensic science and its associated semantics. In Q. Rossy, et al. (Eds.), *The Routledge international handbook of forensic intelligence and criminology*. Routledge, Abingdon, Oxon.
Palmer, G. (2001). A road map for digital forensics research. First Digital Forensics Research Workshop.
Steel, C. (2014). Idiographic digital profiling: Behavioral analysis based on digital forensics. *Journal of Digital Forensics, Security and Law, 9*(1), 7–18.
United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime—Draft. United Nations.

Further Reading

Casey, E., & Rose, C. (2010). Forensic analysis. In E. Casey (Ed.), *Handbook of digital forensics and investigation*. Burlington: Elsevier Academic Press.
Edwards, G. (2020). *Cybercrime investigators handbook*. Hoboken: Wiley.

Investigations: Domestic

Christopher Dowling[1] and Anthony Morgan[2]
[1]Australian Institute of Criminology, Canberra, ACT, Australia
[2]Serious and Organised Crime Research Lab, Australian Institute of Criminology, Canberra, ACT, Australia

Keywords
Abandonment · Abuse · At-fault divorce · Child custody · Children · Divorce · Document review · Domestic investigation · Family · Income · Infidelity · Investigation · Marital assets · Marital finances · Marriage · Matrimonial · No-fault divorce · Private investigator · Spouse · Relationship · Surveillance

Definition

Domestic investigation: the process by which a private investigator collects information to support a client's position in a family or relationship matter, typically concerning at-fault divorce, disputes over marital assets, or child custody arrangements.

Introduction

The stereotype of the private investigator as a disreputable sleuth for hire who catches cheating spouses is still widely held, although it obscures the complicated reality of domestic investigations. While a proportion of private investigators still specialize in these investigations, they now constitute a relatively small proportion of the work undertaken in the private investigation industry (Faber 2013). Furthermore, domestic investigations frequently concern a range of issues outside of infidelity and are overwhelmingly undertaken in a professional and lawful manner to inform legal proceedings around divorce-related disputes (Prenzler 2006). Critically, delving into the private lives of clients and their families is uniquely difficult for private investigators and can intensify already emotionally heightened disputes. Changes to family law systems across the United States and other Western countries regarding marriage and divorce, and the proliferation of certain personal and Internet technologies, have also had implications for the nature and frequency of domestic investigations. This chapter will begin with a brief overview of domestic investigations, before outlining the investigative process and the types of evidence commonly collected. It concludes with a discussion of some of the unique challenges that private investigators regularly encounter when undertaking these investigations, including the emotional nature of this work, the ethical and practical dilemmas inherent to domestic investigations outside of legal proceedings, and the emergence of new technologies.

What Are Domestic Investigations?

The main task for private investigators when undertaking a domestic investigation is to search for and collect information on misconduct or mistreatment within a client's family or marital relationship (Becnel 2017; Gill and Hart 1996; Gill et al. 1996; McMahon 2007; Prenzler 2006). Much of the investigation work undertaken by private investigators throughout the early- to mid-twentieth century focused on uncovering spousal infidelity. This was largely driven by laws at the time requiring spouses to demonstrate some form of marital misconduct or mistreatment in order to obtain a divorce, which frequently amounted to establishing the existence of an extramarital relationship.

From the 1970s, family law systems across the United States and other Western countries gradually introduced options for no-fault divorce, removing the need to demonstrate spousal misconduct or mistreatment (including infidelity) and allowing couples to legally end their marriage when they decide it is no longer worth continuing. Consequently, the demand for domestic investigations focused on infidelity reduced significantly in many Western countries, and less than 5% of private investigators in the United States now specialize in undertaking these investigations (Faber 2013; Gill and Hart 1996, 1997; although evidence suggests that there have been recent increases in demand for domestic investigations of this nature in China and South Korea as social taboos around divorce have subsided, see Jeffreys 2010; Lee et al. 2014). However, although no-fault divorce has become standard, reducing the need for divorce-related domestic investigations, private investigators are still sometimes engaged when at-fault divorce is pursued. While infidelity continues to be the focus of most of these divorce-related investigations, they can also concentrate on uncovering evidence for other forms of marital misconduct and mistreatment, including physical and psychological abuse, or spousal abandonment.

Aside from infidelity and marital misconduct and mistreatment, private investigators are also hired during divorce matters where there is a dispute over marital assets. In these cases, a domestic investigation will focus on uncovering income or other assets concealed by a spouse to prevent their fair distribution across both parties or to avoid paying alimony or child support. Finally, domestic investigations can be initiated where there is a dispute regarding child custody, and a client wants information to demonstrate their former spouse's lack of fitness as a parent.

The goal of a domestic investigation across these different types of matters is to generate evidence that can be used by a client during a legal proceeding, either to ensure a fair distribution of marital assets or to obtain primary or sole custody of children. Importantly, evidence of infidelity and other forms of marital misconduct and mistreatment is now used during at-fault divorce proceedings to support clients who are pushing for more alimony or a larger share of the marital assets, and not to justify the divorce.

While private investigators may be hired to undertake a domestic investigation directly by someone undergoing a divorce-related or child custody dispute, they are more often hired by, and liaise with, the attorneys representing these individuals. As domestic investigations are rarely straightforward, private investigators typically charge hourly rates to undertake them, ranging from US$40 to $200 per hour (PInow 2019). Often this will not include additional costs incurred such as equipment fees (e.g., photos and videos, GPS equipment) and travel and accommodation costs, which clients pay as a flat fee. Clients typically pay a retainer prior to a domestic investigation commencing, and hourly rates and other costs are charged against this, with anything left at the conclusion of an investigation being refunded. The total cost of these investigations varies widely, ranging from around US$300 to over US$1000, while clients can pay retainers of up to US$5000.

The Process of Domestic Investigations

How a domestic investigation is undertaken, and what evidence is collected, will naturally depend on the nature of the matter being investigated (Becnel 2017; McMahon 2007; Nemeth 2010;

Schefcick 2004). Nevertheless, there are a number of investigative techniques that are commonly used as part of these investigations, and they invariably culminate in a brief of evidence comprising critical documents, visual records, interview transcripts, testimonies, and/or investigator reports for use in a legal proceeding.

As in any private investigative work, interviews are often used during domestic investigations (Becnel 2017; McMahon 2007; Nemeth 2010; Schefcick 2004). Interviews with clients in the earliest stages of an investigation are important for establishing the parameters and focus of an investigation (i.e., what the target is suspected by the client of having done and why they suspect it) and for obtaining details and lead on the target that will facilitate further investigative activity. Private investigators may also interview a target's colleagues, associates, and neighbors to obtain investigative leads, while domestic investigations pertaining to child custody disputes often involve investigators speaking with children's teachers and carers. Finally, witnesses to marital mistreatment or misconduct and/or poor parenting practices can be very useful sources of information during these investigations. Aside from establishing the scope of a domestic investigation and providing leads, transcribed interviews and written statements can also form crucial pieces of evidence, both on their own and as supplements to other forms of evidence.

Physical surveillance is regularly undertaken, particularly as part of investigations pertaining to at-fault divorce proceedings and child custody disputes (Becnel 2017; Jeffreys 2010; McMahon 2007; Nemeth 2010; Prenzler and King 2002; Shulman 2000). The goal of surveillance will generally be to observe and record (usually visual) evidence of certain activities engaged in by a spouse, most often infidelity, abuse, or practices that reflect negatively on their fitness as a parent. Preparation is critical before undertaking surveillance. Investigators must know what their target looks like and obtain detailed information on physical characteristics (e.g., hair type and color, eye color, size and physical build, tattoos, and other distinguishing features) and mannerisms prior to commencing any surveillance activity. Other information, such as the target's address, vehicle details, place of employment and other frequented locations, and known associates, is also vital to becoming familiar with likely surveillance sites and paths in advance of actual field work. When infidelity is the focus of investigation, uncovering details of the person with whom a spouse is suspected of having extramarital relations will also aid in the surveillance process, particularly in identifying likely liaison sites and times. Mobile surveillance may be undertaken initially, as an investigator is becoming familiar with the sites and paths frequented by a target and activities performed at these sites. Later, an investigator may undertake a fixed surveillance at a few select locations where she/he believes there is a high probability of obtaining evidence. Importantly, as the information being collected will often be used as evidence during a legal proceeding, its collection and storage must be thorough. Visual evidence must be as clear and unambiguous as possible in whom and what it is showing, and accompanying notes must be detailed.

Reviews of official documents and records are also commonly undertaken as part of domestic investigations (Becnel 2017; McMahon 2007; Schefcick 2004; Shulman 2000). Document reviews are critical to identifying income or assets that have been concealed by a spouse during divorce proceedings and conducting background and character checks on parents to inform assessments of each person's suitability as a custodial parent. Vast amounts of information relevant to these goals can be obtained through document reviews, including full names and dates of birth, social security numbers, education and employment details, possible relatives, current and prior residential addresses, vehicle registrations, voter registrations, business and commercial affiliations, property ownership, credit history, organizational membership, criminal convictions, traffic offenses, and permits held. Much of this data is freely available to the public and can be accessed online or on-site in public libraries, government offices, court houses, and some private sector organizations. Even the target's trash can contain documents useful to these investigations. This information is now also collated in online

subscription investigative databases, allowing private investigators to obtain documents and records from a variety of different sources without having to expend as much time or effort. Of course, as in any investigation that involves collecting documentary information, investigators need to demonstrate its accuracy and verifiability, along with the reliability of its sources.

The Challenges of Domestic Investigations

Domestic investigations can present private investigators with a number of unique practical, ethical, and emotional challenges. Private investigators have noted that domestic investigations can be highly emotional, given their focus on disputes that have serious implications for clients' financial and personal lives (Gill and Hart 1997; McMahon 2007). Many have also noted the risk of clients refusing to accept the outcome of a domestic investigation where findings are not supportive of their predetermined positions. Under these circumstances, it can be difficult for private investigators to remain objective and refrain from becoming emotionally involved in a case. Furthermore, they may feel pressure to violate the law and other ethical/professional standards to collect evidence and push for an outcome they know their client wants (e.g., generating evidence of infidelity through entrapment).

Additionally, private investigators are sometimes asked to undertake domestic investigations outside the scope of those discussed in this chapter. These include background checks on potential suitors a client is dating, investigations of infidelity in nonmarital relationships, and checking for drug use or other misbehaviors by clients' children (Prenzler 2006). Critically, while not illegal, some private investigators consider these investigations in breach of their professional codes of conduct and refuse to undertake them, as they do not inform a legal proceeding of any kind and involve invading an individual's privacy purely to satisfy a client's personal curiosity (Becnel 2017). Given the occurrence of these investigations outside of any formal legal proceeding, there is also much more ambiguity around the standard of proof that must be met for a client's suspicions to be considered supported.

Finally, new technologies have introduced a number of challenges, but also opportunities, for private investigators undertaking domestic investigations. As discussed, the growth of the Internet has brought with it a proliferation of databases that collate personal information from various sources that investigators would previously have had to locate and search manually. This has greatly reduced the time and effort required by private investigators to undertake domestic investigations, particularly those concerning disputes over marital assets, but carries with it the need to carefully discern reliable and up-to-date databases from those with less reliable or outdated information. Additionally, the proliferation of mobile phone technology and social media in particular has presented private investigators undertaking investigations into infidelity and other relationship issues with a wealth of potential information and leads, including records of conversations, photographic/video evidence, and social connections.

Conclusion

This chapter has examined domestic investigations, which private investigators undertake to inform legal proceedings regarding at-fault divorce and legal disputes over marital assets or child custody arrangements. Changes to divorce laws since the 1970s, specifically the introduction of no-fault divorce, have greatly reduced the demand for these investigations in the United States and other Western countries, although they remain the specialty of a small proportion of private investigators and continue to play an important role in the outcome of some divorce-related legal proceedings. Many of the investigative techniques and information sources used by private investigators as part of other types of investigations (i.e., interviews, physical surveillance, and document reviews) are employed when undertaking domestic investigations. Importantly, domestic investigations frequently require private investigators to navigate a number of unique

practical, ethical, and emotional challenges. These include the painful and distressing nature of what is typically investigated (e.g., infidelity, abuse) and of the potential implications of these investigations for clients (e.g., loss of child custody), requests to undertake investigations outside of formal legal proceeding, and the proliferation of certain information technologies, which have created both challenges and opportunities for private investigators.

Cross-References

- ▶ Interviewing Adults: Communication at the Front Line
- ▶ Interviewing Children
- ▶ Law: Administrative
- ▶ Private Detectives

References

Becnel, P. A. (2017). *Introduction to conducting private investigations: Private investigator entry level (02E)*. Dublin: Coventry House Publishing.

Faber, K. (2013, November 5). *The 10 most common specialties of private investigators*. Retrieved from https://www.pinow.com/articles/1737/the-10-most-common-specialties-of-private-investigators

Gill, M., & Hart, J. (1997). Exploring investigative policing: A study of private detectives in Britain. *British Journal of Criminology, 37*(4), 549–567.

Gill, M., & Hart, J. (1996). Historical perspectives on private investigation in Britain and the US. *Security Journal, 7*(4), 273–280.

Gill, M., Hart, J., & Stevens, J. (1996). Private investigators: Under-researched, under-estimated and underused. *The International Journal of Risk, Security and Crime Prevention, 2*, 187–200.

Jeffreys, E. (2010). Regulating private affairs in contemporary China: Private investigators and policing of spousal infidelity. *China Information, 24*(2), 149–167.

Lee, C. H., Lee, C. M., Choi, J. H., Lee, J., & Hong, E. P. (2014). Factors affecting likelihood of hiring private investigators (PI): Citizens' traits and attitudes toward police and PI. *International Journal of Law, Crime and Justice, 42*, 188–202.

McMahon, R. J. (2007). *Practical handbook for private investigators*. Boca Raton: CRC Press.

Nemeth, C. P. (2010). *Private security and the investigative process*. Boca Raton: CRC Press.

PInow. (2019, January 22). *How much does a private investigator cost?* Retrieved from https://www.pinow.com/articles/261/private-investigator-cost

Prenzler, T. (2006). Private investigators. In M. Gill (Ed.), *Handbook of security* (pp. 423–437). London: Palgrave Macmillan.

Prenzler, T., & King, M. (2002). *The role of private investigators and commercial agents in law enforcement* (Trends and issues in crime and criminal justice no. 234). Canberra: Australian Institute of Criminology.

Schefcick, P. E. (2004). *The information seeking behavior of private investigators: A study of investigators in North Carolina and Georgia (unpublished master's thesis)*. Chapel Hill, NC: University of North Carolina.

Shulman, D. (2000). Professionals' accounts for work-related deceptions. *Symbolic Interaction, 23*(3), 259–281.

Further Reading

Sennewald, C. A., & Tsukayama, J. K. (2015). *The process of investigation: Concepts and strategies for investigators in the private sector*. Oxford: Elsevier Inc.

Standler, R.B. (2012). *Privacy violations during divorce in the USA*. Accessed at: http://www.rbs2.com/dprivacy.pdf, March 6, 2019.

Investigations: Employee Theft of Employer Property

Clarissa Meerts
Faculty of Law, Department of Criminal Justice and Criminology, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Keywords

Asset misappropriation · Employee theft · Internal investigations · Corporate investigations

Definition

Stealing, Use or misuse of an employer's property or assets by an employee without permission.

Introduction

Employee theft of employer property is a major issue for organizations (see, e.g., a 2017 article on. com, claiming a 50 billion loss per year for US businesses). Even though the general scope of the problem seems apparent, exact numbers of

employee theft are difficult to obtain. The dark number for employee theft is high. One reason for this is the fact that much employee theft goes undetected or is erroneously defined as another loss (▶ Retail Shrink). It may, for example, be unclear whether an item is stolen or just lost and if stolen, whether it was stolen by an employee or a customer (▶ Consumer Retail Shoplifting). Another reason, however, is that many employers decide not to report the theft to the police, investigating the matter themselves instead (Meerts 2018b). This contribution starts with a discussion of the issue of employee theft, after which investigations into employee theft are discussed.

Employee Theft: Definitions and Types

As mentioned above, theft of employer property by their employees is a major issue for organizations. "Theft" or "asset misappropriation" can be defined in a narrow and a broad way. In its yearly "report on the nations," the Association for Certified Fraud Examiners (ACFE) divides asset misappropriation into the general categories "cash" and "inventory and all other assets" (2018: 11). Under the banner of asset misappropriation of "inventory and all other assets," one can place both tangible and non-tangible assets. In a narrow definition, theft is about the misappropriation of tangible property. In a broader definition, employee theft also includes non-tangible assets, such as money stored on a bank account or even time. Other forms of employee crime, such as workplace violence, employee theft of employee property, or corruption/bribery, are not within the scope of this contribution but may be very harmful to an organization and individual victims nonetheless.

The theft of tangible objects may be small-scale and low-impact (e.g., in the case of employees occasionally taking office supplies such as stationary home) but may also involve large-scale theft, theft of very valuable property (e.g., laptops), or theft of (large amounts of) cash. Theft of employer property is, however, just one of the multiple ways in which an employee may enrich himself or herself at the detriment of the employer. Another common form of employee theft is asset misappropriation in the sense of fraud or embezzlement. This type of employee theft is concerned with the theft of an organization's assets by people who are entrusted with the management of such assets. Strictly speaking, theft of cash from a cash register and fraud through false reimbursement fall under the banner of asset misappropriation. However, the most damage is done when asset misappropriation concerns the theft of money through virtual cash flows. This last type includes famous examples of rogue traders, e.g., Nick Leeson (Leeson and Whitley 1996), accounting fraud, e.g., Enron (McLean and Elkind 2013), and embezzlement, e.g., Bernie Madoff (Van de Bunt 2010).

Another manner in which employees may commit theft against their employer is theft of "time" or of services. In such a case, services provided by the employer or the time for which the employer pays is used inappropriately. This may be through the falsification of billable hours (stating more hours were worked than was the case in actuality), or the employee may, for example, use company time for personal activities. Many employees, for example, use social media at work, but this also includes behavior that is commonly considered inappropriate, e.g., watching porn at work. In case of "theft of time," the line between employee *crime* and behavior that is *undesirable* but not criminal gets blurry (more on this below).

Another harmful form of employee theft of employer property is the theft of ideas. Through, for example, corporate espionage, intellectual property might be stolen by employees, selling it to competitors or even states. This type of employee theft often causes much damage.

Employee Theft: Perpetrators

Employee theft may be committed by employees from all levels of an organization. Lower-level employees and middle and upper management are all involved in different types of employee theft of employer property. The type of theft and the damage caused by it depend on the position of the employee (ACFE 2018). The well-known saying "opportunity makes the thief" is relevant in this context. Theft of cash is more

likely in the case of those employees who handle cash (cashiers, lower management), while misappropriation of "virtual" assets can only be done by employees (often managers) who are in a position to sign off on financial decisions. It has been suggested that the response to the instance of employee theft is dependent on the position of the employee within the organization as well: in case of lower-level employees, organizations tend to more often report officially to the police than when it comes to employees who have a higher (and, importantly, more sensitive) position within the organization (Meerts and Dorn 2009). We now turn to these reactions to employee theft.

Investigations into Employee Theft: Public or Private?

The security landscape can be divided into different security providers (see also ► "Police: Public Versus Private Policing"). Security may be provided by the state (► Public Policing), by private security providers or by public/private partnerships (see ► Security: Concepts and Definitions). Investigations into theft of employer property are in many cases not executed by the criminal justice system (Button et al. 2015). For several reasons, organizations tend to not report internal crime to the police (Williams 2005; Meerts 2018b). For one, reporting to law enforcement authorities inevitably leads to a loss of control over information flows and over the process of the investigations. Criminal investigations can do much damage to the reputation and to the day-to-day processes of an organization. Secondly, criminal justice investigations often do not lead to an outcome that is very useful for an organization. Many reports by organizations to the police are not investigated, and further along the line in the criminal justice system, the prosecution office might decide not to prosecute, or a judge might not deem guilt proven. But even if a case is investigated and prosecuted and a guilty party is punished, the punishment that follows will not solve the problem of the organization. The employee is not fired by a criminal prosecution, and the stolen assets are often not recovered and returned to the organization. Furthermore, criminal justice solutions are notoriously slow. All of this makes a report to the police quite an inefficient step from the organization's point of view. Relatedly, there is a low level of confidence among organizations with regard to the problem-solving capabilities of the criminal justice system. A final reason for organizations not to report is that the criminal justice system only deals with a limited scope of behaviors: only those that fall within the reach of criminal law may be investigated and prosecuted through the criminal justice system. This means that those types of employee misbehavior that are undesirable but not criminal cannot be reported to the law enforcement authorities.

The above considerations lead to the situation in which many instances of employee theft are not reported to, or investigated by, law enforcement authorities. Instead, organizations often investigate employee theft or fraud themselves (through their in-house security department) or contract corporate investigators to do so (Meerts 2018a). These (internal or external) corporate investigators do not have powers of investigation, available to the police, but their position to the organization gives them much access to information within the company. As an employer, the organization has access to much information about their employees. This means that corporate investigators can use information derived from internal systems (including communication systems such as email), internal documents (such as financial administration), and open sources (such as the Internet). Even though corporate investigators do not have the legal power to interrogate an employee, they may interview him or her, and although an employee's cooperation is voluntary, the employer may attach consequences (such as dismissal) to noncooperation.

Many instances of employee misconduct are thus investigated privately (Gill 2013). After such an investigation, a report to the authorities may still be made; however, many employers opt for a private solution (Button et al. 2015). Solutions can be sought within the private legal sphere in numerous ways. Employee theft of employer property may be settled in civil court, through a civil suit to reclaim damages or to terminate the labor agreement. Additionally, the labor contract may be ended through the use of

employment regulations, and internal regulations can be used to discipline the employee. Many (large) organizations have a system of discipline in place, which can range from administering a warning to a summary dismissal (Meerts 2018a). In this way, the problem for the organization may be solved in an efficient way, allowing the organization to act swiftly and move on.

Conclusion

Employee theft of employer property, defined as "stealing, use, or misuse of an employer's property or assets by an employee without permission," is a serious problem for organizations. Theft can take many shapes and sizes and may be committed by a variation of employees in different positions within an organization. While it is known that many organizations make an effort to prevent employee theft through prevention measures and private security solutions (such as the use of ▶ "Security Guards: Authority and Power", ▶ "Physical Security: Video Surveillance, Equipment, and Training", and ▶ "Cybersecurity: Preparedness"), it is often assumed that when a crime does occur, the investigations of it will be handled by the criminal justice system. However, much of the investigations into and solutions sought for employee crime remain entirely in the private sphere. This leads to a situation in which it is very difficult to provide a meaningful estimation of the scope of the problem of employee crime.

Cross-References

- ▶ Bribery
- ▶ Corporate Security
- ▶ Investigations: Consumer Retail Shoplifting
- ▶ Investigations: Criminal
- ▶ Investigations: Fraud
- ▶ Interviewing Children
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Police: Public Versus Private Policing
- ▶ Public-Private Partnerships: Security Organizations
- ▶ Retail Security: Employee Theft
- ▶ Security: Concepts and Definitions
- ▶ Workplace Violence: Assault

References

AFCE. (2018). *Report to the nations. 2018 global study on occupational fraud and abuse*. Austin: Association of Certified Fraud Examiners.

Button, M., Wakefield, A., Brooks, G., Lewis, C., & Shepherd, D. (2015). Confronting the "fraud bottleneck": Private sanctions for fraud and their implications for justice. *Journal of Criminological Research, Policy and Practice, 1*(3), 159–174.

Cnbc.com (2017, September 12). This crime in the workplace is costing US businesses $50 billion a year. https://www.cnbc.com/2017/09/12/workplace-crime-costs-us-businesses-50-billion-a-year.html

Gill, M. (2013). Engaging the corporate sector in policing: Realities and opportunities. *Policing, 7*(3), 273–279.

Leeson, N. W., & Whitley, E. (1996). *Rogue trader: How I brought down Barings Bank and shook the financial world*. Boston: Little, Brown & Company.

McLean, B., & Elkind, P. (2013). *The smartest guys in the room: The amazing rise and scandalous fall of Enron*. New York: Penguin.

Meerts, C. A. (2018a). *The semi-autonomous world of corporate investigators. Modus vivendi, legality and control*. Rotterdam: Erasmus universiteit Rotterdam.

Meerts, C. A. (2018b). The organisation as the cure for its own ailments: Corporate investigators in the Netherlands. *Administrative Sciences, 8*(3), 1–15.

Meerts, C. A., & Dorn, N. (2009). Corporate security and private justice: Danger signs? *European Journal of Crime, Criminal Law and Criminal Justice, 17*(2), 97–111.

van de Bunt, H. (2010). Walls of secrecy and silence. *Criminology & Public Policy, 9*, 435–453.

Williams, J. W. (2005). Reflections on the private versus public policing of economic crime. *British Journal of Criminology, 45*(3), 316–339.

Further Reading

Henry, S. (1983). *Private justice. Towards integrated theorising in the sociology of law*. London: Routledge & Kegan Paul.

Kennedy, J. P. (2017). Functional redundancy as a response to employee theft within small businesses. *Security Journal, 30*(1), 162–183.

Traub, S. H. (1996). Battling employee crime: A review of corporate strategies and programs. *Crime & Delinquency, 42*(2), 244–256.

Walby, K., & Lippert, R. (Eds.). (2014). *Corporate security in the 21st century: Theory and practice in international perspective*. Basingstoke: Palgrave Macmillan.

Investigations: Environmental Pollution Dumping

Rifath Ali and Troy Rawlins
Department of Safety, Security, and Emergency Management, College of Safety and Justice, Eastern Kentucky University, Richmond, KY, USA

Keywords

Environmental pollution dumping investigations · Environmental pollution studies · Environmental pollution types · Anthropogenic pollution · Environmental stressors · Pollution dumping · Pollution forms · Pollution sources · Pollution pathways · Pollution dissipation · Pollution sectors · Air pollution · Water pollution · Radioactive pollution · Soil pollution · Noise pollution · Light pollution · Thermal pollution · Scotopic sky brightness · Land pollution · Sanctioning strategy

Definition

Pollution is the introduction of human-made, physical, and chemical substances into the environment that cause harm to people and other living organisms. Commonly, pollution results from people interacting with the environment, and those human activities pollute the environment, adversely affecting drinking water, soil, and air. Investigation of environmental pollution dumping is a fact-gathering process to determine whether pollution was intentionally dumped with indifference to the law and/or the harm that pollution actually or potentially causes.

Introduction

This entry describes the areas and factors by which investigations determine how environmental pollution became concentrated, known as *pollution dumping*. *Anthropogenic* pollution is environmental pollution caused in nature by humans or human influence, and it affects every living organism. Since 1950, 140,000 new pesticides and chemicals have been created by manufacturing companies, some of which are toxic, such as hydrochlorofluorocarbons (HCFCs), polychlorinated biphenyls (PCBs), and dichlorodiphenyltrichloroethane (DDT). Unfortunately, many of these chemical pollutants are being dumped into the environment, causing areas to become oversaturated (Arora et al. 2018). Investigative processes address pollution dumping for each of the following seven types of environmental pollution – air, water, radioactive, soil, noise, light, and thermal.

Environmental Pollution

There are seven recognized forms or *types* of pollution: air, water, radioactive, soil, noise, light, and thermal. Pollution dumping resulting these pollution types can be waste in the form of solid, liquid, gas, or energy. Solid waste is merely solid material discarded as useless, such as non-recyclable and non-biodegradable materials. Liquid pollutants include industrial wastewaters and human sewage. Greenhouse gasses are comprised of methane, carbon dioxide, and nitrogen oxides. Noise pollution is energy in the form of sound pressure levels that disturb daytime communication and nighttime rest. Light pollution is the obstructive illumination of nature, including hindering the night sky view. Thermal pollution equates with global warming, resulting in an increasing temperature in nature.

The investigation focus of environmental pollution dumping is referred to as the *source*. Generally, pollution is caused by human activity and can be categorized as either a *point source* or *nonpoint source*. The point source is the origin of a specific pollution dump that can be located. Alternatively, a nonpoint source has no boundary. Known as *diffuse pollution*, its origin is difficult to pinpoint. Unclean river water is considered diffuse pollution if the pollution dumping source cannot be identified. Investigations have determined that sources of river water pollution can

be domestic, such as bathrooms and kitchens, or that the pollution dumping is from industry, agriculture, and/or transportation (Munafo 2005).

Associated with each source of pollution is its *pathway*, or *route of entry*, to the recipient. The pathway identifies how the pollutant travels from the source into the environment and then how it contacts the human body or another recipient. The *effects* of toxic pollution dumps dissipate with *dispersion*, *dilution*, *deposition*, and/or *degradation*. Investigations into active pollution dumping incidents seek to confirm that the impact is mitigated as (a) smoke disperses into the air and away from the source, (b) liquid and soluble pollutants are diluted, (c) suspended solids are deposited on river beds, or (d) the composition of the pollutant breaks down (Woodrow et al. 2018).

Finally, our natural resources of water, air, soil, and land are negatively impacted by pollution. Depending on the type of pollution, these sectors are affected in different ways. Investigations have shown that deliberate pollution dumping sites are locally unwanted land uses (LULUs). In the United States, when population centers are near LULUs, they are usually low income and often non-white communities. Ecological awareness in the general population is high in negatively impacted regions, but environmental concerns in society-at-large for those living in environmentally at-risk areas are minimal (Bullard 2000). *Not in my backyard* (NIMBY) has emerged as an effective response strategy against localities and companies who try to engage in pollution dumping in rural, destitute areas. Environmental pollution dumping investigations are often associated with NIMBY campaigns (Bullard 2000). In the rest of this entry, the seven types of pollution are described along with how they are investigated in terms of source, pathway, and consequences.

Air Pollution

Air pollution is the contamination of natural air with harmful vapors, fumes, and chemicals. Causes of this pollution dumping into the atmosphere include vehicle gas emissions, burning materials, and harmful industrial by-product fumes (Arora et al. 2018).

Globally, air pollution contributes to atmospheric changes but has a *nonpoint source* that is difficult to isolate worldwide. Locally, however, air pollution dumping often has a *point source* that is known by nearby resident populations. Common local sources of air pollution dumping include wood and charcoal burning by households, small businesses, manufacturing, and vehicles. Air pollution is not always visible or odorous. Deadly carbon monoxide and dangerous carbon dioxide, usually nonpoint sources, are invisible and odorless gasses.

Local investigations manage these environmental situations since the polluting businesses impact all households in the region, regardless of culture or development level. An investigation into tropical streams showed that warmer temperatures have affected macroalgae, which in turn have caused changes in the fish physiology and diversity (Rolla et al. 2009). Investigations have also shown that a consequence of dumping harmful chemicals into the atmosphere as pollutants, such as carbon dioxide, pollution, increases climate change (Zinabu and Pearce 2003).

When the concentration and toxicity of air pollutants are high, the effects are worse for the environment, making it difficult to eradicate particularly following seasonal or natural changes. Higher concentrations of air pollution dumping result in breathing issues for anything alive. Additional effects of air pollution include increases in smog prevalence, acid rain, higher asthma incidences, and crop depletion from less oxygen. Then, as a result of environmental risk factors due primarily to air pollution, health-care costs increase at an alarming rate (Arora et al. 2018).

Water Pollution

Water pollution is contamination by pollutants that decrease water purity, characterized by excess chemical or biological substances causing harm to living organisms. Biological water pollutants are microorganisms responsible for waterborne diseases and thus are harmful to all life forms. If not contained and treated, feces from infected organisms allow pollutants to seep into the surface and groundwater. Sometimes a *nonpoint source* of water pollution occurs as illegal dumping in

rivers, lakes, oceans, and underground reservoirs. This water pollution dumping then affects these water sources, as well as soil moisture and groundwater in aquifers. Next, the now-polluted rivers flow into the ocean and damage the marine environment. Dispersion in large bodies of water dilutes the pollutant, so the most significant harm is at the river mouth. Symbolized by large oil spills and groundwater oil seepage, water pollution is one of the most dangerous types of pollution because it decreases the available drinkable water and irrigation supply (Arora et al. 2018).

Industry environmental regulations, promulgated by Congress and enforced by the US Environmental Protection Agency (EPA), are established to protect the water supply from toxic chemical pollution dumping. Investigations and research have shown that rigorous environmental regulation does not damage industrial competitiveness. In investigating corporate compliance with the rules, Michael Porter saw that innovation and technology led to "improved competitiveness" (p. 115) in avoiding pollution dumping. Over the years as a result of local environmental pressure, Dow Chemical closed wastewater evaporation ponds and redesigned its processes, costing the company $250,000 but saved $2.4 million per year in reducing toxic pollution dumping by 6,000 tons annually (Porter and van der Linde 1995).

Oversight and investigations of industrial by-product dumping in groundwater, streams, lakes, and oceans remain an ongoing effort, as other water pollution dumping approach their limits. USA Today reported that a 600,000 square mile patch of plastic trash twice the size of Texas is floating in the Pacific Ocean. The mass dumping of plastic with its subsequent coagulation and environmental pollution is destructive, beginning with marine life but eventually trickle back to human (Eriksen et al. 2014). Water pollution dumping investigations and research are being done because additional data regarding the consequences is needed.

Chemical pollutants also include heavy metals, pesticides, and other persistent pollutants. Heavy metals are a group of toxic chemical pollutants that contain compounds of persistent metals such as mercury, cadmium, lead, and chromium. The concentration of heavy metals in water in excess of acceptable levels can cause illness and death among animals and humans, if consumed through drinking and food (Zinabu and Pearce 2003). According to Förstner and Wittmann (2012), the first trace metal aquatic pollution investigations on lakes were done in 1973 in Germany. Practices determining the concentration of heavy metals concluded the level of arsenic decreased with water depth, but the concentration of chromium increased. Investigations found the metal concentration increase in living water organisms was relative to time, seasonal variations, and the initial level of metal distribution in the organism. Marine life near the surface, closer to other pollution-dumping sectors, was more contaminated (Förstner and Wittmann 2012).

Radioactive Pollution

One of the most dangerous types, radioactive pollution is defined as the increase in natural radiation levels caused by human activities. Handling and processing of radioactive materials and storing radioactive waste are extremely dangerous, causing congenital disabilities, cancer, and health deterioration (UNEP n.d.). A *point source* that diffuses more slowly than other types of pollution dumping, radioactive pollution causes include nuclear power plant accidents, incorrect nuclear waste disposal, and nuclear storage leaks. Investigations improved safety and disposal procedures, and the nuclear fallout resulting from explosive testing has decreased since the 1970s, but environmental radioactive pollution dumping is still negatively impacting marine organisms (Kennish 2017). An investigation into a Mayapuri, India, radiation incident revealed the source as contaminated scrap metal from a Delhi University chemistry lab irradiator had been sold, dismantled, and distributed. Eight people were hospitalized as a result of the radiation exposure; one of them died (Yardley 2010).

Soil Pollution

Soil pollution, known as land pollution, contaminates and then hinders plant and animal biological life. Linked to water pollution, soil pollution

causes include non-sustainable farming practices, hazardous waste, and its seepage into the soil, mining, and littering. In addition to poisoning of nearby land and water, soil pollution causes reduced agriculture yields. Soil pollution is a point source, depleting the land of nonrenewable resources, diminishing biodiversity, and gathering harmful, unmanageable chemicals. Investigations discovered that liquid wastes from latrines or industrial waste storage containers flow with pathogenic microorganisms and toxic chemicals onto the land surface and slowly seep into the soil, permeating and contaminating groundwater. Leachate is the result, which percolates into the soil with its toxic, polluting chemicals (Arora et al. 2018). The United Nations manages and mitigates environmental pollution collaborative processes. According to the UN Atlas of the Oceans (2016), degradation of oceans and seas nearshore has polluted land, reducing crop yields and resulting in ecological damage. The negative changes involve atmospheric and sediment flow changes and habitat loss. Mitigation resulting from investigations included cleanup responses and management closure or restriction reprimands (UN Atlas of the Oceans 2016). Ecological strategies for a framework to investigate pollution were proposed in 1980s, beginning with comparing, contrasting, and evaluating pollution detection processes. Interpreting pollution, such as identification and species impact, was the next step, followed by prediction (Underwood and Peterson 1988). MIT led a recent multicity investigation into land-based urban stormwater management, as opposed to underground pipes that have leached pollution into the soil. The investigation found that land-based runoff is sustainable, decentralized, and more easily manageable by institutional mindsets with sustainable objectives (Schulman 2018).

Noise Pollution

Noise pollution is created by human activity disrupting the lifestyle or ability to work in an affected area. Noise pollution dumping can originate with loud music events, airplanes, traffic, railroads, or fireworks. Temporary or permanent loss of hearing can harm wildlife. Noise pollution is generally a point source unless an entire community or region is inundated with the same disruptive sound source (Stansfeld and Matheson 2003). The LIFE MONZA project aim was to establish a methodology to investigate the annoyance factor relative to noise pollution – Methodologies for Noise Low Emission Zones. But the process and results were not authoritative since annoyance is a feeling and its subjective nature cannot be captured in a questionnaire (Arcangeli et al. 2018).

Light Pollution

Light pollution is an obstructive, illuminating point source that prevents the natural from occurring, such as insects navigating correctly and the prey defenses of bats (Gaston et al. 2013). Investigative research has shown that light pollution dumping occurs in large, modern urban centers. Light pollution interferes with nesting sea turtles along a beach highway as well as hindering specific investigative tasks, such as astronomical observation. If the stars cannot be seen, the area is polluted with light (Longcore and Rich 2004). Light pollution dumping is obstructing man's attempt to study nature, a spectral investigation sought to measure the impact of "sky glow" in reducing the ability to see more of the night sky. Results showed that the amplified visual glow from LED lighting has increased the dimmed, *scotopic* sky brightness to where 70% of Americans and more than 50% of Europeans cannot see the Milky Way (Luginbuhl et al. 2013).

Thermal Pollution

Thermal pollution, a nonpoint source, is an increase in temperature in nature occurring over a specific period of time. The heat is often due to carbon gasses trapped from air pollution. Deforestation, a high regional carbon footprint, and power plants can cause temperatures to rise. Slight fluctuations are normal, and life can adapt, but quick changes in nature's temperature cause the water supply to diminish and a loss of wildlife. Global warming has resulted in warmer oceans and oceanic thermal expansion, thus reducing land availability (Arora et al. 2018). Studies, rather than investigations, are ongoing, measuring

the impact of thermal pollution on the environment. Global warming is responsible for decreasing the permafrost region by up to 35%, releasing pathogenic bacteria and viruses that have been buried until now (Wright 2017).

Conclusion

Human action initiates pollution, the result of which can cause additional pollution. All pollution is interconnected, so sustainable strategies are needed that address affected environment sectors at the source. For example, *municipal solid waste* (MSW) impacts all sectors – water, soil, and air. MSW is the accumulation of everyday items that are discarded by the public as trash. Systems addressing MSW in large, industrialized Asian cities combine four methods to achieve optimal management results: analysis, data acquisition, mathematical projection, and identification. With identifiable domestic and industrial point sources, the pollution effects dissipate when separated from large urban centers because the pathway to recipients is controlled. A study of Bangalore, India, results, with both door-to-door and *community bins* (CB) collection, revealed that overall expenses decreased with an increased CB pickup rate (Mondal et al. 2018). This investigation outcome is key because it underscores the importance of municipalities proactively addressing a pollution dumping challenge.

Pollution exacts a heavy toll on nature and life in general but especially upon the immediate population. "Personal efficacy," according to Bullard (2000), is the needed response adopted in recent years to cope with *environmental stressors*. Stressors include municipal solid waste facilities, industrial plants with chemical emissions, toxic waste dumps, and hazardous waste landfills. Disproportionately, as mentioned previously, those most directly impacted by pollution dumping tend to be low income and a different race or culture. The decision to speak out against what is happening to those affected in their backyard is a difficult one. Investigations with the social justice movement have raised awareness and are well documented. More investigations and research to support the body of evidence, however, are needed for the environmental advocacy movement. *Problem-focused coping* is the approach that directly addresses the pollution dumping issue with facts, receives media coverage, and is subject to peer review in the community. Not only in poor, rural areas but everywhere, people are taking note of what is happening in their backyard and taking action (Bullard 2000).

In addition to local investigations and activism oversight pertaining to environmental pollution dumping, compliance enforcement provides the regulatory control. Furthermore, Keith Hawkins proposed decades ago, after a 30-month study, that the social definition of pollution provides a strong "accusatory and adversarial" deterrent to being a polluter. He called this a *sanctioning strategy*. Private companies, as well as public and government entities, understand the importance of inhibiting pollution dumping to avoid public scrutiny (Hawkins 1984). Going forward, contemporary investigations will be central in recognizing successful efforts to mitigate and reduce the impacts of environmental pollution dumping.

Cross-References

- ▶ Critical Infrastructure: Water and Wastewater Systems Sector
- ▶ Hazardous Environmental Effects
- ▶ Investigations: Criminal
- ▶ Investigations: Terrorism

References

Arcangeli G, Mucci N, Giorgi G, et al. (2018). 566 Evaluation of quality of life and annoyance in the context of life monza project. *Occupational and Environmental Medicine*, *75*(A518). Retrieved from https://oem.bmj.com/content/75/Suppl_2/A518.2

Arora, N., Fatima, T., & Mishra, I. et al. (2018). Environmental sustainability: Challenges and viable solutions. *Environmental Sustainability*. https://doi.org/10.1007/s42398-018-00038-w

Bullard, R. (2000). *Dumping in dixie: Race, class, and environmental quality* (3rd ed.). Boulder: Hachette Book Group/Westview Press.

Dhasmana, A. et al. (2019). Scope of nanoparticles in environmental toxicant remediation. In: R. Sobti, N. Arora, & R. Kothari (Eds.), *Environmental biotechnology: For sustainable future*. Singapore: Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-981-10-7284-0_2

Environmental Pollution Centers. (n.d.). What is radioactive pollution? Retrieved from https://www.environmentalpollutioncenters.org/radiation/

Eriksen, M., Lebreton, L, & Carson, H, et al. (2014). Plastic pollution in the world's oceans: More than 5 trillion plastic pieces weighing over 250,000 tons afloat at sea. *PLoS ONE*. https://doi.org/10.1371/journal.pone.0111913

Förstner, U., & Wittmann, G. (2012). *Metal pollution in the aquatic environment*. New York: Springer Science & Business Media.

Gaston, K., Bennie, J., Davies, T., & Hopkins, J. (2013). The ecological impacts of nighttime light pollution: A mechanistic appraisal. *Biological Reviews, 88*(4), 912–927. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1111/brv.12036.

Hawkins, K. (1984). *Environment and enforcement: Regulation and the social definition of pollution*. Oxford: Clarendon Press.

Kennish, M. (2017 updated). Practical handbook of Estuarine and marine pollution. Boca Raton: CRC Press.

Longcore, T., & Rich, C. (2004). Ecological light pollution. https://doi.org/10.1890/1540-9295(2004)002[0191:ELP]2.0.CO;2

Luginbuhl, C. B., Boley, P. A., & Davis, D. R. (2013). The impact of light source spectral power distribution on sky glow. *Journal of Quantitative Spectroscopy & Radiative Transfer*. Retrieved from https://ac.els-cdn.com/S0022407313004792/1-s2.0-S0022407313004792-main.pdf?_tid=5b54b4c6-30ad-468b-954c-82b552d0d9c2&acdnat=1548561090_f546a8d77cbbdd029d8c37b82f50d4d2

Mondal, M., Speier, C., & Weichgrebe, D. (2018). Multistage optimization approach for sustainable municipal solid waste collection systems in urban areas of Asia's newly industrialized countries. *Environmental Management*. https://doi.org/10.1007/s00267-018-1130-6

Munafo, M. (2005). River pollution from non-point sources: A new simplified method of assessment. *Journal of Environmental Management, 77*(2), 93–98. https://doi.org/10.1016/j.jenvman.2005.02.016

Open University. (2016). Pollution: Types, sources and characteristics. Retrieved from http://www.open.edu/openlearncreate/mod/oucontent/view.php?id=79946&printable=1

Porter, M., & van der Linde, C. (1995). Toward a new conception of the environment-competitiveness relationship. *Journal of Economic Perspectives*, *9*(4), 97–118. Retrieved from https://www.aeaweb.org/articles?id=10.1257/jep.9.4.97

Rolla, A., Esteves, K., & Avila-da-Silva, A. (2009). Feeding ecology of a stream fish assemblage in an Atlantic Forest remnant (Serra do Japi, SP, Brazil). *Neotropical Ichthyology*. Retrieved from http://www.scielo.br/scielo.php?pid=S1679-62252009000100009&script=sci_arttext&tlng=es

Schulman, A. (2018). Sustainable cities and institutional change: The transformation of urban stormwater management. DSpace@MIT. Retrieved from https://dspace.mit.edu/handle/1721.1/118076

Stansfeld, S., & Matheson, M. (2003). Noise pollution: Non-auditory effects on health. *British Medical Bulletin, 68*(1), 243–257. https://doi.org/10.1093/bmb/ldg033

UN Atlas of the Oceans. (2016). Pollution and degradation. Topic 774. Retrieved from http://www.oceansatlas.org/subtopic/en/c/774/

Underwood, A. J., & Peterson, C. H. (1988). Towards an ecological framework for investigating pollution. *Marine Ecology, 46*(1), 227–234. Retrieved from https://www.jstor.org/stable/24827587?seq=1#page_scan_tab_contents.

UNEP. (n.d.). Radioactive substances. *United Nations Environment Programme*. Retrieved from http://www.cep.unep.org/publications-and-resources/marine-and-coastal-issues-links/radioactive-substances

USA Today. (2018, March 22). World's largest collection of ocean garbage is twice the size of Texas.

Woodrow, J., Gibson, K., & Seiber, J. (2018). *Pesticides and related toxicants in the atmosphere. Reviews of environmental contamination and toxicology*. New York: Springer.

Wright, P. (2017). Thawing permafrost could unleash ancient, dangerous diseases, scientists say. Retrieved from https://weather.com/science/environment/news/2017-11-08-thawing-permafrost-release-diseases/

Yardley, J. (2010). Scrap metal radiation raises concerns in India. *The New York Times*. Retrieved from https://www.nytimes.com/2010/04/24/world/asia/24india.html

Zinabu, G., & Pearce, N. (2003). Concentrations of heavy metals and related trace elements in some Ethiopian rift-valley lakes and their in-flows. *Hydrobiologia, 492*(1–3), 171–178. Retrieved from https://link.springer.com/article/10.1023/A:1024856207478.

Further Reading

Scope of nanoparticles in environmental toxicant remediation (2019) by Anupam Dhasmana and editors Swati Uniyal, Vivek Kumar, Sanjay Gupta, Kavindra Kumar Kesari, Shafiul Haque, Mohtashim Lohani, and Jaya Pandey. From Environmental Biotechnology: For Sustainable Future. The article studies the need to quicken the sanitization of contaminated sites and reduce best practice methods costs.

Practical Handbook of Estuarine and Marine Pollution by Michael J. Kennish. Recently updated, the handbook addresses all types of environmental pollution dumping. Updated Dec 2017, 1st Edition 1996. Taylor & Francis Group, CRC Press imprint

Investigations: Firearms

Michelle D. Miranda
Farmingdale State College, The State University of New York, Farmingdale, NY, USA

Keywords
Firearm · Gun · Ammunition · Gunshot residue · Chemistry · Ballistics · Shooting reconstruction · Forensic · Investigation

Definition

Breech the rear end of the barrel where the cartridge is inserted

Class characteristics identifying features of an object based on comparison to known standards or an established set of criteria

Individual characteristics features of an object that distinguish it from objects in the same class

Muzzle the front end of the barrel from which the projectile emerges

Introduction

Investigations related to firearms include forensic firearms examinations, gunshot residue analysis, wound examinations, and shooting reconstructions. Forensic firearms examinations encompass the analysis of the firearm and ammunition, such as firearms operability testing, microscopical bullet and cartridge case comparisons, and serial number restorations. Gunshot residue examinations consist of the chemical, microscopical, and spectroscopic examinations of residues that result from discharge of the ammunition within the firearm, specifically the primer and gunpowder. Gunshot residue examinations are often conducted to determine a muzzle-to-target distance or estimate a maximum distance at which a firearm will cease to deposit residues on a target. Examination of gunshot wounds can further assist in investigations, providing information about the nature of injuries sustained by a surviving shooting victim or the cause and manner of death of a decedent. The latter determinations are done during an autopsy and may include mapping the wounds and determining the trajectory of the projectile(s) within the body during external and internal examinations, respectively. The culmination of data obtained through the examinations of the firearms and ammunition, gunshot residue analysis, and wound patterns combined with trajectory analysis (often broadly referred to as "ballistics") at the crime scene aid in the overall goal of developing a shooting reconstruction. These shooting reconstructions further incorporate information obtained during the course of the broader investigation and may include blood pattern analysis, recognition and examination of physical traces, recovery of digital traces, witness statements, and any matters related to standard forensic and police investigation methods.

Ballistics is the study of a projectile's movement from the trigger pull through to the projectile's interaction with the target. Internal ballistics occurs within the firearm when the firing pin strikes the cartridge and all subsequent events until the projectile exits the muzzle end of the barrel. External ballistics is concerned with the actions of the projectile from the moment it exits the firearm and travels a path for some distance until the projectile reaches the target. This involves any potential interactions of the projectile with intermediary objects or surfaces. These interactions may result in changes in the speed, direction, or overall behavior of the projectile. Terminal ballistics includes the interaction of the projectile with the target. Trajectory analysis takes into consideration all three types of ballistics with the goal of developing a shooting reconstruction.

Most importantly, each individual phase of firearms investigations (from the initial examination of the scene to the laboratory analysis) and the overall interpretation of resultant facts to develop a reconstruction of events are scientific endeavors (De Forest 2005). The fundamental basis for such forensic investigations is that activities such as shootings will generate traces which can be recognized, collected, and analyzed by qualified scientists with the ultimate goal of applying logical

reasoning and critical thinking to the consideration of alternate hypotheses, contextualizing events, and providing a meaningful interpretation of events to aid in fact-finding endeavors. Firearms investigations, in part or as a whole, are subjected to evidence admissibility requirements (e.g., the Frye, the "Daubert trilogy" or the Federal Rules of Evidence guidelines in the United States of America) and therefore should be conducted with scientific rigor, transparency, and neutrality.

Firearms and Ammunition

The legal definition of a firearm may vary from one jurisdiction to another. According to 18 U.S. Code § 921 (3), "the term firearm means (A) any weapon (including a starter gun) which will or is designed to or may readily be converted to expel a projectile by the action of an explosive; (B) the frame or receiver of any such weapon; (C) any firearm muffler or silencer; or (D) any destructive device. . ." [Supplemental definitions are provided for a destructive device (18 U.S. Code § 921 (4)) and a firearm muffler/silencer (18 U.S. Code § 921 (24))]. Firearms can be classified as handguns or long guns. Handguns can be further subdivided into revolvers and pistols, and long guns can be subdivided into rifles, shotguns, submachine guns, and machine guns. Firearms that are homemade are generally referred to zip guns, and firearms may be modified, such as a sawed-off shotgun or through the addition of a muzzle/flash suppressor. Handguns, rifles, submachine guns, and machine guns have a rifled barrel consisting of a series of lands and grooves along the length of the barrel produced during manufacture. The method of producing the rifling can vary, with some methods imparting characteristic tool marks along the barrel (Rowe 1988). This rifling imparts a spin to the bullet, and it is these marks that can be transferred to the bullet as it travels down the barrel when a firearm is discharged.

The primary components of ammunition are the case, the primer, the propellant, and the projectile (bullet), which can be collectively referred to as the cartridge. One purpose of the cartridge is to expand and seal the rear of the firearm during firing in order to prevent the escape of gases and overall loss of pressure from the breech end of the barrel. As pressure increases within the cartridge, the bullet is forcibly released from the cartridge and the projectile is propelled down the barrel, exiting at the muzzle end of the firearm. Each component of the cartridge can vary in physical or chemical properties.

The case can differ in physical characteristics, such as shape and primer location, features which are used to classify the ammunition. For example, cartridge cases can be described as straight, bottlenecked, or tapered and can be further described as rimmed, semi-rimmed, rimless, rebated, or belted. In general, cartridge cases are brass (an alloy of copper and zinc). The location of the primer within the cartridge can vary, with rimfire and centerfire being the most common types of cartridges. Rimfire cartridges contain the primer spun into a circular rim at the edge of the case, and centerfire cartridges have a primer cup inside the center of the cartridge case. The primer cup holds the priming mixture within the base of the cartridge case. Centerfire cartridges can be further subdivided into Boxer or Berdan priming systems, depending on the location of the anvil, which is the metal component associated with the primer cup (Heard 2013). Upon trigger pull, the firing pin of the firearm will strike the primer cup and the priming mixture will be crushed against the anvil, whether it is contained within the primer cup (Boxer) or incorporated into the case (Berdan). This friction will result in an explosion within the cartridge, which will ignite the propellant (gunpowder). The propellant will burn at a controlled rate, which depends on its quantity, shape, size, and chemical composition.

The projectile, or bullet, is defined by its caliber, which corresponds to the diameter of the bullet. Bullets can vary in shape (e.g., round nosed, elongated, or hollow point) and the presence, absence, and type of jacketing (e.g., non-jacketed, semijacketed, full-metal jacket). The core of the bullet is often lead and the jacketing bronze (copper–tin alloy). Projectiles may also be polymer coated, frangible, or "green" (nontoxic) depending on the intended purpose of the

ammunition, each of which will result in variation to the chemistry and physical characteristics of the projectile and overall ammunition composition. In addition, bullets may contain cannelures, grooves around the bullet that hold lubricant and seat the bullet within the cartridge case.

Shotgun ammunition (shells) contains the head (brass), the primer, a tube (which can be plastic or paper), gunpowder, the wad, the projectile(s), and may contain buffering material. The wad seals and separates components of the ammunition, and can vary in its composition, which may be paper, plastic, or cardboard. The projectile can be either a single rifled slug or spherical pellets of varying size and weight (referred to as the shot, which can be further classified as birdshot or buckshot depending on the diameter of the pellets). The buffering material is a polymer that may be added to the shot in an effort to minimize pellet deformation. In shooting cases involving shotguns, components of the ammunition may be found at the scene, adhering to a target surface, or within the shooting victim.

Forensic Firearms Examinations

Forensic firearms examinations encompass the analysis of the firearm and ammunition, such as firearms operability testing, microscopical bullet and cartridge case comparisons, and serial number restorations. Examinations in the forensic firearms laboratory include physical examination and classification of the firearm, and additional analysis may include function (dry fire) testing; trigger pull testing; evaluation of malfunctioning, damaged, modified, homemade, or antique firearms; and shooting-related tests such as muzzle-to-target determinations, cartridge case ejection pattern determinations, body armor tests, and test bullet recovery. In addition, firearms examinations may include the utilization of databases for bullet and cartridge case comparisons and gun linkages, such as the Integrated Ballistics Identification System (IBIS).

Prior to forensic firearms examinations, the examiner should consider the presence and recovery of traces from the firearm and any associated ammunition. These traces can include fingerprints, blood spatter, tissue or bone fragments (which may be present on the exterior of the firearm or within the barrel), and any other microscopical traces that may be adhering thereon (such as hairs, fibers, glass, etc.). The firearm should be examined visually and stereomicroscopically in an effort to record its gross physical features. The examiner may note characteristics such as color, make, model, manufacturing markings (such as serial numbers, proof marks, part numbers, and country of origin), caliber (the measurement from land to land for a rifled barrel) or gauge, type of firearm (action; single or double), ammunition type and capacity (which includes the examination of the magazine, if present), size (length of barrel and overall length of the firearm), rifling characteristics (e.g., polygonal), and the presence, absence or modification of safety features. Examiners should look for and document faulty components, damage, alterations, or wear to the firearm.

Microscopical analysis of ammunition may be based on bullet comparisons or cartridge case comparisons, depending on the items recovered during the investigation and submitted to the laboratory for analysis. These examinations are conducted with a comparison microscope, that is, two microscopes attached by a bridge that allows for simultaneous viewing of both objects when viewed through the oculars. Comparisons can be between projectiles or cases recovered from the scene (unknowns), between test fires (knowns), or between knowns and unknowns in an effort to establish common origin (to link a projectile or a cartridge to a particular firearm). This is based on the premises that (1) the firearm may impart characteristics from the barrel onto the bullet as the bullet travels down the barrel after discharge and prior to exiting the firearm and (2) the firearm may impart characteristics from the breech face and/or firing pin onto the cartridge case upon depression of the trigger and the force of the discharge process.

Examinations are conducted on both intact bullets (that may or may not be damaged or distorted) and fragments of the bullet core or jacket. With bullets, the examiner will evaluate

class and individual characteristics, and note features such as caliber and general rifling characteristics. Specifically, the examiner may note the degree and direction (left or right) of twist, number and width of the lands and grooves, and the depth of the grooves on the bullet as well as any additional markings or imperfections that may be traced to a particular firearm. For cartridge cases, the examiner will evaluate headstamp information located on the base of the cartridge case to determine caliber and manufacturer and will look for the presence of marks that would result from cycling, chambering, extraction (extractor marks), ejection (ejector marks), and impacts with the breechface and the firing pin. The breechface and firing pin impressions will be examined in detail in an effort to locate class and individual characteristics that can be compared between cartridge cases. Prior to the preparation of the projectile for comparison microscopy, the bullet should also be examined for the presence and recovery of any adhering traces. The analysis of biological traces utilizing serological and DNA methods may provide investigatory information about the trajectory of the projectile including its interaction with an individual. The detection and examination of nonbiological traces may further provide information about the path of the bullet and its interaction with intervening targets, such as clothing (fibers or a fabric impression), a wall or door (paint, plaster, sheet rock, wood), a vehicle (glass, paint, metal), or the ground (plant matter, soil, asphalt). It should be kept in mind that anything can be an intervening object, and based on Locard's exchange principle, the object and the projectile can transfer material from one to the other (Petraco and De Forest 1990).

Serial number restoration may be conducted in a forensic firearms laboratory in an effort to restore defaced firearms. Firearms may be defaced using a variety of methods, such as gouging, grinding, or over stamping. Various regents, including acid solutions, may be utilized for chemical restoration along with abrasive cloths of varying coarseness for polishing of the defaced area. Prior to application of restoration methods, the examiner should visually inspect the defaced area in an effort to determine the possible method of obliteration and to remove any potential traces that were deposited during the defacement. Determining the method of obliteration may aid in determining the best methods for successful restoration. The serial number can be used to track the provenance of the firearm, from manufacturer to ownership.

Gunshot Residue Analysis

Gunshot residue examinations consist of the chemical, microscopical, and spectroscopic examinations of residues that result from discharge of the ammunition, specifically the primer and gunpowder. Gunshot residue examinations are often conducted to determine whether or not someone may have discharged or handled a recently discharged weapon, a muzzle-to-target distance, or a maximum distance of deposition. In addition, gunshot residue analysis methods may be employed to determine if a projectile came into contact with a surface. Such examinations will look for chemical components consistent with bullet "wipe" or "splash," which can include residue from the bullet (copper, lead), lubricant from the ammunition, and residue from the barrel that is transferred to the bullet in addition to adhering residues from the primer and propellant.

Gunshot residues are often divided into inorganic and organic residues, with the organic residues being a combination of products from the individual components of ammunition ejected from the muzzle end of the firearm upon discharge (directed toward the target) and inorganic residues being largely derived from the primer and exiting toward the rear and sides of the firearm (generally directed toward the shooter). These latter primer residues are often analyzed in "shooter's hands" cases to determine if an individual recently fired, handled, or was in the vicinity of a discharged firearm. Despite the name, collection of samples is not restricted to the shooter's hands, and may include the face, hair, and clothing of the suspected shooter as well as objects in the vicinity of the shooting. The elemental composition of these samples has historically been analyzed

using atomic absorption spectroscopy (AAS) and scanning electron microscopy-energy dispersive x-ray spectrometry (SEM/EDX). The SEM/EDX is more commonly utilized because in addition to elemental data, the instrumentation also provides critical morphological characteristics of the primer residues, which is important during the interpretation phase of analysis (Zeichner 2009).

The basis for inorganic gunshot residue testing is the chemistry of the primer. The primer is composed of a combination of an initiating explosive, an oxidizing agent, a fuel, sensitizers, frictionators, and binding agents. Compositions may vary and also include dyes or proprietary components. SEM/EDS analysis is based on detecting the most commonly encountered elemental profile in standard ammunition, specifically lead, barium, and antimony resulting from lead styphnate (initiating explosive), barium nitrate (oxidizing agent), and antimony sulfide (fuel), respectively. A characteristic primer residue particle consists of barium, antimony, and lead and has spherical morphology. Additional guidelines and standards have been established for classifying and interpreting resultant elemental and morphological data in primer residue cases (see, for example, ASTM E1588-17 2017).

Gunshot residue analysis can also be conducted in an effort to determine a muzzle-to-target distance or estimate a maximum distance at which a firearm will cease to deposit residues on a target. The premise is that the size of the residue pattern is a function of distance and both the firearm and ammunition employed; as the distance between the muzzle and target decreases, the size (diameter) of the pattern will decrease and the concentration of residues deposited on the target will increase. The generation of these residues is largely based on the chemical composition of the propellant, although residues that exit the muzzle end of the firearm could also come from the primer or the bullet as well as from the firearm itself, which may contain lubricants, residue from cleaning products, and general build-up of soot and materials within the barrel ("fouling"). Traditional black powder (a mixture of potassium nitrate, charcoal, and sulfur) ammunition has been replaced by black powder substitutes and the more common smokeless powder, and ammunition can vary in smokeless powder composition – single based (nitrocellulose), double based (nitrocellulose, nitroglycerine), and triple based (nitrocellulose, nitroglycerine, nitroguanidine). Smokeless powder may also consist of various additives, such as coatings, stabilizers, plasticizers, lubricants, and dyes, some of which may be proprietary and unique to a manufacturer. Smokeless powder can be further characterized by its morphology and size, making microscopical examination of powder particles to determine physical characteristics an important aspect of gunshot residue examinations. The most common colorimetric methods for resolving gunshot residues on targets (often conducted on victim's clothing) are dithiooxamide/rubeanic acid for the detection of copper, sodium rhodizonate for the detection of lead, and the modified Griess test for the detection of nitrites. Additional analytical methods have been employed to detect and identify gunshot residues, including Fourier transform infrared spectrometry (FT-IR), x-ray fluorescence (XRF), gas chromatography (GC), liquid chromatography (LC), and capillary electrophoresis (CE) (see Dalby et al. 2010 for a review of literature pertaining to gunshot residue analytical methods).

Several factors can influence the deposition and retention of gunshot residues (Nichols 2004). Interpretation of gunshot residue patterns requires consideration of intervening targets, the handling of objects containing the residues, and modifications to the firearm, such as the addition of a muzzle/flash suppressor. The detection of gunshot residues and distance determinations can also be conducted with shotgun pellet patterns, making gunshot residue examinations useful for both handguns and long guns. The size of the shotgun pattern is primarily controlled by the distance (range) and choke (muzzle diameter) of the gun while the number of pellets is controlled by the gauge and load of the shell used.

Shooting Reconstructions

The culmination of data obtained through the battery of tests conducted during forensic firearms examinations, gunshot residue analysis, wound

interpretations obtained from the shooting victim (s), and trajectory analysis at the crime scene contribute to the overall goal of developing a shooting reconstruction. Shooting reconstruction at the scene includes documenting bullet holes, utilizing trajectory rods or lasers to trace the pathway of the bullet, and examining physical traces such as bloodstains and digital traces such as CCTV footage. Additional scene work may also include determining the sequence of shots within a target (e.g., a series of shots in a vehicle windshield) and shot accounting, or "reconciling the number of fired cartridge cases, fired bullets, bullet holes (in inanimate objects), and bullet wounds" (Hueske 2006, p. 248). Additional information can be ascertained from the detection of gunshot sounds based on witness statements or gunfire detection technologies (Haag and Haag 2011). Information derived during detection and investigation, such as witness statements and reviews of phone records, are also incorporated into the reconstruction effort with the goal of developing a timeline of events.

External and internal examinations of the shooting victim can aid in determining entry and exit wounds as well as the pathway of the projectile(s) within the body (DiMaio 2016). Examinations of the body can be aided by obtaining x-rays to locate projectiles, whether intact or fragments. These projectiles can subsequently be recovered and submitted to the forensic firearms laboratory for microscopical examination and comparison. From such data and the examination of physical traces at the scene, it may be possible to determine position and location of the shooting victim(s) at the time of the incident. Trajectory analysis involves understanding the nature of the projectile in flight. The bullet travels a curved path and is subjected to external forces such as air and gravity (Rinker 2007). Interior forces of pressure and energy, which are functions of the individual ammunition components as well as the firearm, will also impact the trajectory of the projectile. As the bullet interacts with different surfaces, the trajectory, speed, and behavior of the bullet may change. One aspect of trajectory analysis is ricochet analysis, which deals with the rebounding of the bullet off of a hard surface that may result in an angular (directional) change in the bullet's trajectory. By examining the location of a projectile recovered at the scene or in a victim and evaluating the trajectory of the projectile(s) including any factors that may contribute to changes in the path of the bullet (such as the aforementioned intervening targets and ricochets), it may be possible to determine the approximate location of the shooter during the incident. Such information can be further supported by considering cartridge ejection patterns and the location and distribution of gunshot residues.

Conclusion

Firearms investigations are multifaceted and complex. Whether investigating an apparent suicide, a police-involved shooting, or a mass shooting, there are many layers to the process of developing a shooting reconstruction to determine a sequence of events. During the initial crime scene investigation, evaluation and preliminary interpretation of the scene as traces are being collected for further laboratory analysis is imperative to develop and refine hypotheses and consider alternate hypotheses for evaluation. The importance of educated, well-trained scientists at such complex scenes is critical and essential. Shooting reconstructions require consideration of myriad examinations including identification and testing of the firearm(s) involved, microscopical analysis and comparisons of ammunition, gunshot residue analysis, victim wound analysis and interpretation, and overall trajectory analysis. Reconstructions should set out to determine the locations and movements of the shooters and the victims, the weapons used in the shooting, and any additional information that may accurately recount the shooting event. By utilizing data from the examinations, it may be possible to reconstruct the events so as to support or refute the accounts of witnesses or suspects.

Cross-References

▶ Criminals: Active Shooters
▶ Investigations: Criminal

References

18 U.S. Code § 921. Definitions.
ASTM E1588-17. (2017). *Standard practice for gunshot residue analysis by scanning electron microscopy/energy dispersive x-ray spectrometry.* West Conshohocken: ASTM International.
Dalby, O., Butler, D., & Birkett, J. (2010). Analysis of gunshot residue and associated materials – A review. *Journal of Forensic Sciences, 55*(4), 924–943.
De Forest, P. (2005). Crime scene investigation. In L. Sullivan & M. Rosen (Eds.), *Encyclopedia of law enforcement* (pp. 111–116). Thousand Oaks: SAGE.
DiMaio, V. (2016). *Gunshot wounds*. Boca Raton: CRC Press.
Haag, M., & Haag, L. (2011). *Shooting incident reconstruction* (2nd ed.). San Diego: Academic.
Heard, B. (2013). *Forensic ballistics in court*. West Sussex: Wiley.
Hueske, E. (2006). *Practical analysis and reconstruction of shooting incidents*. Boca Raton: CRC Press.
Nichols, R. (2004). Gunshot proximity testing: A comprehensive primer in the background, variables and examination of issues regarding muzzle to target distance determinations. *AFTE Journal, 36*(3), 184–203.
Petraco, N., & De Forest, P. (1990). Trajectory reconstructions I: Trace evidence in flight. *Journal of Forensic Sciences, 35*(6), 1284–1296.
Rinker, R. (2007). *Understanding firearm ballistics* (6th ed.). Clarksville: Mulberry Publishing.
Rowe, W. (1988). Firearms identification. In R. Saferstein (Ed.), *Forensic science handbook, volume II*. Englewood Cliffs: Prentice Hall.
Zeichner, A. (2009). Forensic aspects of firearm discharge residue analysis. In R. Saferstein (Ed.), *Forensic science handbook volume III*. Englewood Cliffs: Prentice Hall.

Further Reading

Association of Firearms and Toolmark Examiners (ATFE), AFTE Journal archives.
Goddard, C. (1926). Scientific identification of firearms and bullets. *Journal of the American Institute of Criminal Law and Criminology, 17*, 254–263.

Investigations: Fraud

Chelsea A. Binns
John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Fraud · Investigations · Investigative process · Insider threat · Fraud examination · Investigative plan · Evidence collection · Follow the money · Intelligence gathering

Definition

A fraud investigation is a thorough and objective, fact-gathering process conducted to determine whether or not a fraud-related crime was committed. Evidence is collected during this process to establish facts, inform findings, protect victims, and build a case which may potentially culminate in a criminal and/or civil action.

Introduction

Fraud investigations are a specific type of investigation conducted to determine whether a fraud-related crime was committed. Public attention to the phenomenon fraud investigations increased following a series of public company frauds in the early 2000s (Coenen 2009, xv). Many of those crimes are listed among the "Ten Biggest Frauds in Recent U.S. History" and include Enron in 2001, Tyco International and WorldCom in 2002, and HealthSouth in 2003 (Forbes 2017).

There are many different types of frauds in existence. Overall, there are types of frauds that can be perpetrated across several industries, such as check fraud, and frauds that can be specific to an industry, such as healthcare fraud. Here, the focus is on occupational fraud. Occupational frauds are those committed by an employee, to the detriment of the organization (ACFE). In that realm, the primary types of occupational fraud are corruption, asset misappropriation, and fraudulent statements (ACFE).

Fraud investigations should commence with careful background research and the creation of an investigative plan. Careful planning is critical to the success of a fraud investigation. Once the investigation commences, investigators will determine the best approach, based on information gleaned during the planning phase. Next, evidence is collected, with a keen eye toward "following the money." Intelligence is gathered to gain additional insight, with an eye toward potential litigation. The ultimate goal is a detailed case file, documenting all information gathered.

While many similarities in investigative practices exist across all investigations, fraud

investigations have specific challenges. One is a time crunch. There is a certain haste to solve a fraud-related crime, in order to prevent further victimization. Another is the complexity associated with fraud matters. Fraud schemes can be complicated, and the documentation involved can be voluminous. Thus a fraud investigation might require the assistance of one or more experts. For this and other reasons, one seasoned investigator said he would rather work on a homicide case than a fraud investigation (Giacalone 2015). Yet with the proper planning, investigating a fraud case can be a rationalized and rewarding experience.

Fraud Investigation Resources

One leading authority on conducting fraud investigations is the Association of Certified Fraud Examiners (ACFE). The ACFE, founded in 1988, is the world's largest anti-fraud organization and provider of anti-fraud training and education. As of this writing, they have over 80,000 members, globally. Their mission is to reduce the incidence of fraud and white-collar crime and to assist the Membership in fraud detection and deterrence (ACFE 2018). The ACFE categorizes a fraud investigation as one of the four basic components of a general fraud examination. The other three components of a fraud examination are financial transactions and fraud schemes, law, and fraud prevention and deterrence (ACFE 2014). They also provide a detailed guide for fraud examiners called the "Fraud Examiners Manual" to assist investigators in conducting their investigations.

Fraud Investigation Practices

Planning Phase

To begin, the investigator should meticulously plan his/her case. Fraud investigations should be approached as any other investigation would – as "an impartial, non-judgmental, fact-gathering process" (Biegelman and Biegelman 2010, p. 296). The early steps are critical to the success of a fraud investigation (Biegelman and Biegelman 2010, p. 296). Investigators should conduct an initial review of the available documents to determine the fraud allegations. A more detailed review will occur later, as the investigation progresses.

Today, the types of documentation available to investigators is vast. In the corporate setting, "documentation" may include but is not limited to "contracts, invoices, correspondence, memoranda, weekly reports, presentations, telephone messages, emails, reports, performance reviews, performance improvement plans, medical records, and other written or recorded material" (ACFE 2014, p. 3.118). Investigators may also want to obtain credit statements, bank accounts, and social media posts (Giacalone 2015). It is important for investigators to ensure that all data, especially electronically obtained data, is saved, secured, and documented in the case file (Giacalone 2015).

From the documents, the investigator should gain a thorough background of the allegations. A keen understanding of the allegations will be important in the development of the investigative plan. From the documents reviewed, investigators will learn the resources required to conduct the investigation (Biegelman and Biegelman 2010, p. 296).

At this time, the investigator should determine the type of fraud that may have occurred. This information will help the investigator to develop the appropriate team to assist in the investigation. Depending on the allegations, fraud investigators may require the expertise of auditors, attorneys, fraud examiners, managers, and security personnel, among others (ACFE 2014, p. 3.128). The investigative team will also include partners in federal, state, and/or local agencies, depending on the type of fraud-related crime uncovered (Giacalone 2015).

Investigative Plan

Before commencing a fraud investigation, the investigator should develop an investigative plan. Generally speaking, most investigative plans will include a framework for the use of financial, personnel, and technological resources.

Each member of the investigative team should be invited to contribute to the plan. Their active participation in the plan will be prosperous for the overall investigation (ACFE 2014, p. 3.135). In the corporate setting, an investigative plan will need to be cleared/approved by in-house counsel and/or retained outside counsel (Biegelman and Biegelman 2010, p. 296).

The investigative plan can help with the investigation by ensuring an established strategy is in place, with adequate resources to accomplish the investigative tasks. The organization that retained investigative services may have a specific framework that should be followed. This can serve as a guide through the investigative planning process. Investigative steps may include "intake, assignment, assessment of the allegation, creation and approval of the investigative plan by legal counsel, investigation, reporting, disciplinary action and remedial steps to improve internal controls and policy breakdown" (Biegelman and Biegelman 2010, p. 296). Potential witnesses may also be identified at this stage, as planning might be required to connect with those witnesses. However, more witnesses are likely to be identified as the investigation progresses.

The investigative steps in the plan may include identifying the goals of the investigation, the parties who need to be kept informed, the scope of the investigation, the investigation timeframe, the need for law enforcement assistance, operational issues, the course of action, and the necessary resources (ACFE 2014, p. 3.136).

The investigative plan should include a chronology of events, leading up to the fraud. This timeline should include details concerning the victim and suspects. Through this process, inconsistencies can be gleaned. Ultimately, a well-crafted investigative plan might reveal unexpected information. For instance, sometimes the "victim" is actually the fraudster (Giacalone 2015). For this reason, investigators should be sure to keep an open mind when analyzing the chronological data.

An investigative plan is a wise investigative tool. Planning the investigative process in advance can save time and money. The investigator may realize she/he needs additional people or assets to achieve investigative goals. This can be mapped out in the plan. However, the investigator will likely be working within a defined budget. As a result, there may never be enough time or money to accomplish all investigative goals. Compromises may have to be made. This can be realized during the investigative planning process.

Investigative plans may reveal the need for experts and/or technological resources. Experts might be required to advance a specific investigative goal. For instance, the financial expertise of an expert might be necessary to decipher complicated financial transactions. A technology expert and/or software package might be required to analyze encrypted data. These experts often come from the security and law enforcement industry (Pedneault et al. 2012, p. 121). It is important the expert be an ethical, trusted member of the investigative community, to ensure their findings are generally accepted. Upon completion of the plan, the investigator may want to prepare the organization for the upcoming investigation.

Investigation Process

Once the planning is complete, the investigation process may commence. While the general investigative process is similar across disciplines, there are some unique aspects to fraud/financial crime investigations (Pedneault et al. 2012, p. 124). Fraud investigations can be extremely complex. As the investigation progresses, and new information is learned, the investigation will constantly change and evolve (Pedneault et al. 2012, p. 124). As information is uncovered, the original investigative plan might require modification, which is customary.

During this learning process, the investigator develops the perspective from which they will ultimately examine their case. The ACFE advises fraud examiners to investigate fraud from two perspectives: (1) to prove that a fraud has occurred and (2) to prove that a fraud has not occurred (ACFE 2014, Section 3, P. 5). Both scenarios should be explored, in all instances. Why? Because legally, "proof of fraud must preclude any explanation other than guilt" (ACFE 2014, Section 3, P. 5).

Upon commencing a fraud investigation, the ACFE recommends using the "fraud theory approach" (ACFE, Fraud Examiners Manual,

p. 3.106). This approach entails analyzing the available data and developing a theory, or hypothesis, about what may have occurred, based on that information. Once developed, the hypothesis is tested by examining the available data to determine whether it can be proven. If not, that hypothesis is refined, and the process is replicated. As knowledge increases, the hypothesis and theories must be reevaluated (Pedneault et al. 2012, p. 124). It is possible that primary theories will turn into sub theories and alternate theories or may be refuted and become disproved hypotheses (Pedneault et al. 2012, p. 124). New theories may be developed. Ultimately, the hypothesis is continually revised and theory tested via data examination until a fraud is proven, or it is determined that the fraud cannot be proven. Ultimately it will be determined that no fraud was present, or a fraud will be confirmed.

To develop a working theory, investigators will want to gain background information (Pedneault et al. 2012, p. 126). If this industry is new to the investigator, she/he might begin by reviewing publications pertaining to the subject industry. This will allow investigators to develop a working knowledge of the general industry processes and terminology.

Evidence Collection

The general investigation will consist of evidence collection/exhibit preparation, witness identification, document identification, and analysis. Eventually, a suspect may be charged with a crime (Pedneault et al. 2012, p. 123). As a result, it is important to retain and collect evidence with care.

In the corporate setting, electronic evidence may need to be collected from the workplace. A suspect's business activities may require evaluation to determine whether fraud was present. The organization can provide the investigator with this evidence, as the business activities of the suspect/employee are not considered to be private when conducted using business computers/equipment. It is critical that electronically obtained information is obtained, collected, handled, and stored with extreme care. When in doubt, an electronic evidence expert should be contacted to assist (Pedneault 2009, p. 19).

It is important, especially in the corporate setting, to maintain strict confidentiality. Investigative allegations and documentation should be kept private to prevent leaks, reputational damage, tip-off to the fraudster, and erosion of employee confidence (ACFE 2014, p. 3.144). Information should be shared on a "need-to-know basis." Depending on the case, attorney work-product doctrine may apply to the documentary evidence. If the evidence is protected, the subject, government, and third parties may not gain access to this documentation (ACFE 2014, p. 3.148–149).

Electronic evidence may also need to be obtained from a worker's personal electronic devices. If the device was brought into the office, or owned by the organization, they should be involved in this process. Electronic evidence such as bank account activity, or private cell phone records on the part of the suspect, may also need to be obtained. Investigators should consult with the company and law enforcement partners to obtain such evidence, as subpoenas might be required and/or consent from the worker. A review of this evidence might reveal the names of additional witnesses and/or suspects that would not otherwise be gleaned from the available business records.

Additionally, investigators will want to examine the available business records. It is important for investigators to understand the business structure and process (Pedneault et al. 2012, p. 126). Helpful documents include organizational charts, internal policies, and corporate filings. Investigators might also create their own working flow charts, based on their understanding of the business records. In a fraud case, this process might be tedious, involving hundreds or thousands of documents (Johnston 2007, p. 569).

Follow the Money

Upon review, investigators should take note of how money flows within the organization. "Following the money" is an important fraud investigative technique. According to one expert, "the importance in following the money cannot be overemphasized. Whether the case is a simple bank fraud case or a complicated money laundering scheme, when one follows the money, you

will eventually ascertain who is the major player in the fraud" (Johnston 2007, p. 568).

To follow the money, investigators must determine, through a careful review of the financial records, the step-by-step path of the stolen money from "origination to its destination" (Johnston 2007, p. 569). Ultimately, prosecutors will need to demonstrate this process to the judge and/or jury. The prosecution has the burden of proof and must prove each element of the fraud case beyond a reasonable doubt (Johnston 2007, p. 569). Investigators should provide a detailed money trail, ending with the defendant (Johnston 2007, p. 569). Ultimately, the case should be presented to the jury in a "simple, polished and well-organized fashion" (Johnston 2007, p. 569). Visual aids are important in demonstrating the flow of money. Investigators should anticipate this and plan their investigations accordingly.

It is also critical for investigators to understand the parties in their case, including the potential suspect. Investigators can learn more about investigative subjects through the process of intelligence gathering. The intelligence gathering should include a background check on the victim (Giacalone 2015). Ultimately, the victim will be interviewed. The background check will provide the investigator with useful information in advance of the interview. The investigator may strategically choose to reveal or withhold certain intelligence learned during the background check process.

Investigators may conduct an interview of the victim, as part of the investigation. During the interview process, questions should be open-ended and address all of the investigative basics – who, what, where, when, how, and why. Overall, the investigator is looking for the victim to tell a story, and questions should be designed to elicit that story (Giacalone 2015). More detailed follow-up questions can be added later in the interview, to gain knowledge of specifics that may not have been covered during the victim's initial narrative.

Intelligence Gathering

The approaches for additional intelligence gathering include surveillance, database searches, and trash collection (Pedneault et al. 2012, p. 127–131). In a fraud investigation, surveillance can lead to information regarding banking and property ownership. Additional intelligence can be gleaned from Internet databases. Licensed private investigators may gain access to paid databases such as Delvepoint, IRB Research, and TLO which provide a wealth of information on subjects. As assets are uncovered, they may need to be secured, for the purposes of restitution (Pedneault 2009, p. 8).

There are also many publicly available databases that will provide useful information for the investigator. Both sources can provide information to confirm property ownership, including real estate holdings, criminal and civil litigation history, work history, and potential familial and business associates. Trash can also provide useful investigative intelligence. Before proceeding, investigators should check federal and state law. However, it should be noted that case law often sides with the investigator in these matters. While the location of the trash is important, generally speaking, trash is considered to be abandoned property (Pedneault et al. 2012, p. 130–131).

Overall, it is important for investigators to build a thorough and detailed case file. Jurors today have high expectations when it comes to fraud investigations, due to the "CSI effect" (Johnston 2007, p. 566). Specifically, according to prosecutors, jurors, whom have educated themselves in the investigative field via popular crime television shows, can have an inflated standard of proof in fraud matters. This happened during the HealthSouth Corporation fraud matter in 2005. Jurors said they wanted to see HealthSouth CEO Richard Scrushy's fingerprints on the document evidence (Johnston 2007, p. 566). Unfortunately, according to seasoned financial crime investigators, this is an impossible task (Johnston 2007, p. 566). One such expert, James B. Johnston, investigative supervisor at the Essex County Prosecutor's office in Newark, NJ, said he has "never, ever heard of a fingerprint impression having been taken off a piece of document evidence for a fraud case" (Johnston 2007, p. 566). Thus, although jurors might be ultimately disappointed with the evidence in a fraud matter, it is important to consider their high standard of proof when building one's fraud case.

Conclusion

Fraud investigations are detailed and specialized investigations. Careful planning is important to the success of the investigation. Thorough background research is required to conduct a detailed investigative plan. The planning phase helps investigators in determining the best approach. This phase culminates in a detailed investigative plan. The evidence collection process will ideally allow investigators to "follow the money" leading them to the source of the fraud. Intelligence gathering provides additional valuable evidence, which is well documented for potential litigation. Ultimately, a detailed case file is created. This case file is the culmination of a lot of hard work on the part of the investigative team. Special care should be used throughout the investigative process to ensure this file is as detailed, thorough, and accurate as possible.

Cross-References

- ▶ Insider Threat
- ▶ Investigations: Employee Theft of Employer Property
- ▶ Security: Private

References

Association of Certified Fraud Examiners (ACFE). (2014). *Planning and conducting a fraud investigation*. Fraud Examiners Manual.

Association of Certified Fraud Examiners (ACFE). (2018) "Fraud tree." Available at: http://www.acfe.com/fraud-tree.aspx

Biegelman, M. T., & Biegelman, D. R. (2010). *Foreign corrupt practices act compliance guidebook: Protecting your organization from bribery and corruption* (Vol. 8). Hoboken: Wiley.

Coenen, T. L. (2009). *Expert fraud investigation: A step-by-step guide*. Hoboken: Wiley.

Forbes. (2017). "Our take on the ten biggest frauds in recent U.S. history." Available at https://www.forbes.com/pictures/ghde45fli/our-take-on-the-10-bigge/#297a26e37e50

Giacalone, J. L. (2015). Four basic steps in a fraud investigation. *Public Safety Briefing Room.* Lexis Nexis.

Johnston, J. B. (2007). Prosecuting government fraud despite the CSI effect: Getting the jury to follow the money. *New England Law Review, 41*(3), 563–574.

Pedneault, S. (2009). *Anatomy of a fraud investigation*. Hoboken: Wiley.

Pedneault, S., Silverstone, H., Rudewicz, F., & Sheetz, M. (2012). *Forensic accounting and fraud investigation for non-experts*. Hoboken: Wiley.

Further Reading

Pedneault, S. (2010). *Anatomy of a fraud investigation: Fraud detection to prosecution*. Hoboken: Wiley.

Petrucelli, P. R. (2013). *Detecting fraud in organizations*. Hoboken: Wiley.

Wells, J. T. (2014). *Principles of fraud examination* (4th ed.). Hoboken: Wiley.

Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection* (5th ed.). Hoboken: Wiley.

I

Investigations: Money Laundering

John T. Bandler
Bandler Law Firm PLLC and Bandler Group LLC and John Jay College of Criminal Justice, New York, NY, USA

Keywords

Money laundering · Anti-money laundering · Anti money laundering · AML · Terrorism · Terrorist financing · Sanctions · Financial services · Fraud · Theft · Investigations · Prosecution · Financial transactions · Cash · Virtual currency · Digital currency · Bitcoin · Cryptocurrency · Regulation · Criminal statute · Money transmitting · Money remittance · Placement · Layering · Integration · Structuring · FinCEN · Financial Crimes Enforcement Network

Definition

Money laundering is the process criminals use to conceal and disguise the source, destination, or ownership of money and property earned through criminal activity.

Money laundering investigation is the process of identifying money laundering activity for the purpose of stopping it, reporting it to government, or prosecuting it.

Introduction

Money laundering exists because there are successful criminals. Many individuals and organizations commit crime for the purpose of making money, and a considerable amount of criminal activity is conducted for financial gain (OECD 2016). Some criminals are successful in this activity, which means they have the ability to accumulate profits and wealth from their illicit activity. With the prosecution of Al Capone in the 1920s, government realized that one method to identify and prosecute these successful criminal individuals and enterprises was by "following the money." After that, criminals learned they needed to hide and disguise this illegitimate income. The cat-and-mouse investigative game of money laundering – and the investigation of it – was born. Both the government and private sector play significant roles in this investigative process.

In 1986, government realized existing laws were inadequate to address the concealment of illicit income and assets, so criminal money laundering statutes were enacted. Government recognized that it alone could not monitor and investigate financial activity adequately, so duties and responsibilities were placed upon the private sector to detect and combat money laundering. Government created a regulatory and licensing framework to try ensure that only licensed and supervised financial institutions and money service businesses (MSBs) conducted financial transactions on behalf of customers. If individuals seeking to transfer or store funds use banks and money transmitters who are complying with government regulations, then their transactions and activities are being monitored. Government effectively deputized financial institutions to monitor their customers and transactions for suspicious activity that is indicative of money laundering, terrorist financing, or other criminal activity. Entities who fall short on their anti-money laundering (AML) monitoring and reporting can face significant governmental consequences, to include civil fines, loss of license, and even criminal prosecution. If a financial institution loses its license, it cannot continue in business.

In the United States, the Financial Crimes Enforcement Network (FinCEN) is an arm of the Treasury that has responsibility for AML, counter terrorist financing (CTF), and sanctions programs. Sanctions are administered through the Treasury's Office of Foreign Assets Control (OFAC). The anti-money laundering arena overlaps with other areas designed to monitor and restrict the flow of funds. CTF programs seek to restrict and trace the flow of funds to and from terrorists and their organizations. Sanctions programs seek to restrict the ability of individuals, organizations, and nation states who are the subject of sanctions to move and hold funds.

The investigation of money laundering has been, and continues to be, an evolution of laws, regulations, techniques, methods, and technology. On one side are individuals and entities seeking to conceal and disguise funds – criminals, terrorists, sanctioned individuals and countries, or just individuals trying to avoid paying taxes. On the other side are the investigators, regulators, and prosecutors trying to detect this activity. This includes the government and also financial institutions who have invested in AML programs and personnel.

What Is Money Laundering?

As the definition indicated, money laundering is the process of concealing and disguising information about funds earned through criminal activity. It concerns hiding information about one or more aspects of property, such as how it was earned, where it came from, who owns it, and where it is going. It is what prosperous criminals must do in order to maintain their ill-gotten gains and escape punishment. If society wishes to effectively fight the many financial crimes that victimize law abiding citizens, then it needs to address money laundering. Typically, money laundering is described as a three stage process: placement, layering, and

integration (UNODC website, Department of the Treasury, National Money Laundering Risk Assessment 2015).

Placement occurs after criminal activity generates profits, which needs to be placed into the financial system. If the illicit income is cash, then depositing the cash into a bank might constitute placement. Today, large quantities of cash attract unacceptable attention, so cash placement must be done unobtrusively. The criminal could mix the cash with legitimate income from a business that is cash intensive, such as a restaurant, barber shop, pizza parlor, car wash, or other business. Placement could be accomplished through "smurfing," where large amounts of cash are distributed to many individuals ("smurfs"), and all of the individuals deposit small amounts of cash into their respective bank accounts.

Layering is a money laundering process that attempts to disguise and obfuscate the initial placement and true source of the funds. Think of layers of a rotting onion, with each layer concealing the rot within the core. Each layer helps to conceal what is beneath it, so that corrupt income can appear legitimate. One way to layer funds would be to repeatedly transfer money through several shell corporations and countries, another would be to disguise illicit income as the result of a sham transaction, loan, or investment.

Integration is the final money laundering stage where the criminal reaps the illegal reward, such as through the purchase of a home, business, or other investment or asset with funds that appear to be legitimate, untainted by criminal activity. The criminal is now the lawful owner of an asset, with all the accompanying rights.

These three stages are not rigid steps, since the creativity of the criminal is not restricted by definitions and typologies. Further, these stages are well suited for many cash money laundering situations, but with cybercrime and virtual currency new dynamics present themselves. When analyzing money laundering as a criminal offense, remember that terms are specifically defined within the relevant federal or state statute. To commit the crime of money laundering, a person needs to perform specific acts with the appropriate mental state as defined in the particular statute. Generally, someone has committed the crime of money laundering if he or she know funds are criminal proceeds, and conducts financial transactions with these funds for the purpose of concealing or disguising their source, destination, or ownership. (See for example, §§ 18 U.S.C. 1956, 1957). Additional information on criminal statutes appears in the subsequent section "Money Laundering Criminal Statutes."

Who Investigates Money Laundering?

Many different types of organizations investigate money laundering, financial transactions, or the ownership of assets, where facts are not readily apparent or are concealed. Examples include law enforcement, intelligence agencies, regulators, financial institutions, private individuals, journalists, and non-profit organizations. The Treasury Department's Bureau of Financial Crimes Enforcement Network (FinCEN) is a clearing house for financial data and analysis, which is used for both criminal enforcement, regulatory, and intelligence purposes. It is the financial intelligence arm of the US Government, with a mission to keep the financial system from being used for illegal purposes and to promote national security.

Law enforcement investigates suspected violations of criminal money laundering statutes. These investigations are typically complex, so federal law enforcement plays a predominant role in this area. Federal agencies that investigate money laundering include the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Internal Revenue Service (IRS), Department of Homeland Security (DHS), and United States Secret Service (USSS). Violations of federal law are ultimately prosecuted by United States Attorneys (federal prosecutors). State and local law enforcement can also investigate violations of state money laundering laws. The offices of the Attorney General of each state may have the resources to conduct investigations of this type. Some local prosecutors' offices also conduct

significant money laundering investigations and prosecutions, such as the New York County District Attorney's Office. Agencies with a role in protecting the country's national security also analyze financial transactions, including the Central Intelligence Agency (CIA), FBI, DHS, and others. Financial transactions might help reveal nation state espionage, participants in a terrorist cell, or that a nation is evading sanctions.

Financial institutions investigate money laundering. They are required to have anti-money laundering programs which include a compliance officer, policies, procedures, staffing, and tools (see subsequent section on regulation). They need to have adequate ability to detect and investigate suspicious financial transactions, report upon them as required, and properly document their actions. This duty has created the AML profession, designed to keep the institution in compliance with laws and regulation, and to keep the institution from being used as a tool by criminals and money launderers. As a part of these requirements, financial institutions must continually search for and identify money laundering activity, and where found report it to regulators and law enforcement via suspicious activity reports ("SARs") as discussed in the subsequent section. Law enforcement can then investigate – and where warranted and their limited resources allow – bring criminal prosecutions. Financial institutions can terminate relationships with customers whose activity is illegal or suspicious. Government regulators also investigate money laundering and monitor the financial institutions that they supervise to ensure that *they* are properly investigating money laundering. Financial institutions have been deputized by the government to monitor their customers, and regulators are watching the watchers to ensure this is done properly.

Private individuals sometimes probe money laundering. Consider a victim who suffers millions of dollars of damage or losses due to a wrongdoer's theft, misconduct, or negligence. That victim may hire an attorney or otherwise seek a court order directing the wrongdoer to return the funds. The wrongdoer may attempt to hide assets in order to keep them from being seized and may use money laundering techniques. The victim or attorney may hire investigators to try trace and recover funds, to try locate and seize the assets. This investigative process seeks to locate the hidden assets, establish facts that would allow an appropriate court to freeze the assets, and ultimately direct their delivery to the victim. Similarly, journalists scrutinize financial relationships and transactions which may be obscured using money laundering techniques. The phrase "follow the money" was associated with the Washington Post's investigation of President Nixon's Watergate scandal in the early 1970s (All The President's Men 1976). Investigation of financial transactions surrounding Watergate helped piece together who was involved and the breadth of their activities. Many investigative journalists realize the value of financial analysis to uncover facts, motivations, or connections. Examples of nonprofits conducting this type of investigative journalism include Global Witness, the International Consortium of Investigative Journalists, and the Organized Crime and Corruption Reporting Project.

Criminalization, Regulation, and Investigation of Money Laundering

Money laundering has a relatively recent origin as a distinct crime – it was not until 1986 that the first money laundering criminal statute was enacted in the United States, The Money Laundering Control Act, 18 U.S.C. §1956 and §1957. However, the underlying conduct was occurring long before it was explicitly criminalized. Ever since governments have taxed their citizens, some have responded by hiding their money and wealth. Consider Al Capone, the notorious crime boss who settled in Chicago and led the "Outfit" in the 1920s. He led a criminal enterprise that profited handsomely from illegal alcohol transportation and sales (bootlegging), prostitution, and extortion during the prohibition era. To keep his illegal businesses in operation, a host of other crimes were committed, including bribery of public officials, intimidation, assault, and murder. The most serious of these crimes were never successfully prosecuted, perhaps due to witness

intimidation, lack of cooperation, corruption, or an absence of legal tools necessary to hold the crime boss responsible for the physical acts of his employees. Instead, it was tax fraud that ultimately caused Capone's downfall. He did not report his income to authorities, and neither did he sufficiently conceal it, living extravagantly with his riches. Prosecutors proved his failure to report income, and he was sentenced to 11 years prison.

The lesson of Al Capone was not lost on organized crime – unreported income can give rise to prosecution for tax fraud which can mean prison. Further, government might not be content with charging tax fraud. Tracing funds between source and destination might demonstrate the full criminal conduct of the defendant, a leader and profiteer of a criminal operation. To avoid arrest, smart criminals had to disguise some of their illicit criminal proceeds as legitimate income and report this income on their tax returns. Without documented income, they cannot explain expenditures for dinners, cars, boats, and homes. The income must have an appearance of legitimacy, because if the stated activity is truthful they would convict themselves. The tactic of money laundering allowed criminals to earn seemingly legitimate profits, while keeping law enforcement from tracing its true origin. However, it would take more time until government realized this practice needed to be criminalized.

To make criminal profits seem legitimate, "dirty cash" needs to be introduced into the financial system. Dirty cash is inconvenient for many reasons: it is bulky, attracts attention and risk of theft, is hard to store long term, and cannot be used to purchase expensive items such as businesses, houses, cars, and boats. Depositing cash into a bank account allows the criminal to use the financial system to store and transfer funds. Before enactment and proper enforcement of AML laws, criminals might bring tens of thousands of dollars of cash to the bank, deposit it, have their accounts credited, and then funds could be sent by check or wire. Few questions were asked, no reports were filed, and bank employees might have had knowledge about the criminal origin of the funds.

The Bank Secrecy Act of 1970 (BSA) introduced controls to stem this activity, and required financial institutions to detect and report money laundering activity. No longer could a duffel bag of cash be brought to the bank branch and deposited without questions being asked, and without reports being filed. Through the BSA, as it has been periodically amended, banks and many businesses are now required to report cash transactions of $10,000 or more through currency transaction reports (CTRs). They also must detect and report activity indicative of money laundering or other criminal activity through suspicious activity reports (SARs). Failure to make these reports could result in civil and criminal penalties for the bank.

The Money Laundering Control Act of 1986 was another important milestone, marking the first time that the federal government criminalized money laundering. It created new statutes: 18 U.S.C. §1956 and §1957 which made it a federal crime to conduct financial transactions with known criminal proceeds. Many states soon followed with their own money laundering statutes. These laws applied not just to criminals who launder their own ill-gotten gains but to third parties who perform money laundering services for them.

Over the years, there have been various amendments to these laws, including the USA PATRIOT Act of 2001, enacted in response to the terrorist attacks of 9/11. This statute strengthened financial monitoring and penalties, required banks to establish AML and CTF programs, designate a responsible compliance officer, create written policies and procedures, train employees, and obtain an independent audit. Despite the development of laws and regulations, they did not stop money laundering. Instead, criminals continue to seek and develop methods to disguise their activity and evade detection. Investigators need to keep up with emerging trends in order to detect and prosecute offenders.

Virtual currencies – also called digital currencies and sometimes called cryptocurrencies – present new money laundering investigative and regulatory challenges. Most readers have heard of the popular virtual currency Bitcoin. Virtual

currency laundering methods are quite different from cash laundering, since virtual currency is earned, stored, and spent very differently. Criminals, including cybercriminals and identity thieves, have recognized the benefits of virtual currencies for paying each other and for laundering funds. From the creation of the first virtual currency in 1996 until 2013, it was ambiguous as to whether regulation applied to virtual currencies (Bandler, Cybercrime and Digital Currency 2016, p. 9). In 2013 FinCEN made clear that AML and registration regulations did indeed apply to virtual currency issuers and exchangers. However, the effect of this regulatory requirement was limited with the invention of and rising popularity of decentralized cryptocurrencies such as Bitcoin. Virtual currencies can be categorized as centralized or decentralized, where centralized currencies are administered by an entity, and decentralized currencies are typically cryptocurrencies, since it is the blockchain technology pioneered by cryptocurrencies that allows transactions to take place without a central administrator (Bandler, Cybercrime and Digital Currency 2016, p. 3, and ACAMS CAMS Certification Exam Study Guide sixth Ed. 2016, p. 65). With decentralized virtual currencies, there is no central currency administrator to implement an AML program or be held accountable for failing to do so. Thus a review of exchangers and users becomes all the more important. All virtual currencies present money laundering risks because of user anonymity, cross-border value transfer, and limited compliance with regulations and laws. Although virtual currency presents many crime and money laundering risks, investigators should remember that all conventional financial systems and methods also present these risks.

Money Laundering Laws and Regulations

Money Laundering Criminal Statutes

Federal and state criminal statutes prohibit money laundering activity. The applicable federal statutes arose from the Money Laundering Control Act of 1986 as 18 U.S. Code § 1956 (Laundering of Monetary Instruments) and 18 U.S. Code § 1957 (Engaging in monetary transactions in property derived from specified unlawful activity).

18 U.S.C. §1956 provides for penalties of up 20 years federal prison and fines of up to one half million dollars or twice the value of the funds. There are three subdivisions of the crime. Subdivision one sets forth that a person commits money laundering when they have knowledge that property is proceeds of unlawful activity, they conduct financial transactions with these illicit proceeds, and they (i) intend to promote or further more illicit activity, (ii) intend to commit tax fraud, (iii) are trying to conceal or disguise the location, source, ownership, or control of the property, or (iv) are trying to avoid a reporting requirement about the transaction. The transaction "reporting requirements" the statute refers to include the filing of CTRs and SARs, so someone who makes daily cash deposits of $9,000 in criminal proceeds to avoid the $10,000 threshold for the filing of a CTR would have committed money laundering.

Subdivision two of 18 U.S.C. §1956 criminalizes transfer of funds across US boundaries with knowledge that the funds are criminal proceeds, if the transfer is with the intent to avoid a transaction reporting requirement or to conceal or disguise the nature, location, source, ownership, or control of the funds. Bulk smuggling of cash criminal proceeds across the border, or sending a bank wire to disguise the criminal proceeds would be examples of this.

Subdivision three of 18. U.S.C. §1956 is designed for undercover law enforcement "sting" operations. This subsection does not require that the funds *actually* be criminal proceeds, but rather that they were "believed to be" or "represented to be" criminal proceeds. The undercover agent pretending to be a drug dealer who delivers $100,000 in cash to a corrupt businessman or financial advisor may be laying the foundation for a prosecution under this section.

States have statutes that criminalize money laundering. For example, New York State criminalizes money laundering within Article 470 of the state Penal Law. In essence, it is similar to the federal money laundering statute, but it is broken

down into four distinct degrees, distinguished by the amount of funds laundered. Then each degree has multiple subdivisions. Critical aspects include whether the property is the proceeds of criminal conduct, the defendant's intent to promote the carrying on of criminal conduct or engage in tax fraud, and the defendant's knowledge as to whether transactions are designed to conceal or disguise the nature, location, source, ownership or control of criminal proceeds, or avoid reporting requirements.

Money Transmitting Regulations and Criminal Statutes

Every state in the United States except for Montana requires money transmitters within their borders to be licensed by the state. This means that companies within the state in the business of transmitting funds on behalf of customers must submit to state licensure and regulation requirements. Examples of money transmitters include Western Union, MoneyGram, and PayPal.

Consider New York State's Banking Law § 650 (Unlicensed Money Transmitter), which holds that a person or entity who is in the business of sending or receiving money without a license is guilty of a misdemeanor. If the funds exceed certain thresholds – such as $25,000 per month or $250,000 per year – are criminal proceeds – then the offense rises to a felony. With the license come responsibilities to create and maintain records and have an AML program.

Federal law bootstraps upon state money transmitting laws. The federal government can prosecute individuals or entities under federal law if they violate a state money transmitting law. 18 U.S. Code § 1960 (Prohibition of unlicensed money transmitting businesses) criminalizes anyone who knowingly conducts, controls, manages, supervises, directs, or owns all or part of an "unlicensed money transmitting business." An "unlicensed money transmitting business" is one that transfers funds on behalf of customers by any means and either (i) lacks a state money transmitting license where such license is required or (ii) fails to register with the Treasury Department as a money transmitter. *See* 18 U.S.C. § 1960. The registration requirement is set forth in 31 U.S.C. § 5330 (registration of money transmitting businesses).

Thus, compliance with various money transmitting laws requires obtaining a state license, registering with the federal government as a money service business (MSB), creating and maintaining records about the business, customers, and transactions, maintaining an anti-money laundering (AML) program, and reporting required events to FinCEN.

Licensing and Regulation of Financial Institutions

Banks and other financial institutions are common mechanisms for people to store and transmit funds. Like money transmitters, Banks are regulated and licensed. Financial institutions need to be licensed by the state in which they operate, register with the federal government, and are subject to state and federal oversight. They may be supervised by one or more federal organizations, such as the Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of Currency (OCC), National Credit Union Administration (NCUA), Federal Reserve Board (FRB), the Consumer Financial Protection Bureau (CFPB), and FinCEN. State authorities may regulate the bank as well, such as New York's Department of Financial Services.

This licensing and oversight has many purposes, including consumer protection, ensuring the stability of the bank and the financial system, and also anti-money laundering controls (CFPB website, FDIC website, and FinCEN website). Regulations require the institution to have an AML program, which basically means that the bank has policies, people, and systems watching for suspicious transactions and activity indicating criminal activity, money laundering, or terrorist financing.

FinCEN and their Role in AML and Regulation

As mentioned earlier, FinCEN is the bureau within the Treasury Department charged with keeping criminals, money launderers, and terrorists from using the financial system, and with obtaining intelligence from financial transactions.

Under the Bank Secrecy Act (BSA) and USA PATRIOT Act, banks and money transmitters are required to look for suspicious activity and large cash transactions and report it to FinCEN through SARs and CTRs. Every financial institution, money transmitter, and money service business in the USA must comply with regulations, and this includes having an AML program and filing these reports when required. These regulations apply to not only financial institutions but to car and boat dealers, casinos, and art and jewelry dealers. Any business that receives over $10,000 in cash in connection with a transaction needs to file IRS form 8300 with FinCEN or the IRS. All of this information that FinCEN keeps is tightly controlled, and unauthorized disclosure is a serious criminal offense. FinCEN's information is used by criminal investigators and prosecutors at the federal and state level, and by our national security apparatus.

The AML Program

The laws and regulations designed to keep the financial system clean requires that financial institutions and money transmitters have an AML program (Bank Secrecy Act). This means they must create policies, procedures, systems, and employ people to monitor customers, the funds they store and transmit, and investigate potential money laundering activity. It also means that if they fall short of their responsibilities, there can be serious consequences, to include civil fines, criminal prosecution, and loss of license.

The AML program starts with learning who the customer is and what their business is. This is known as "know your customer" (KYC) and customer due diligence (CDD). It requires training employees such as bank tellers and relationship managers to look for signs of money laundering, and it means monitoring all transactions, which might require using special software designed to detect patterns and relationships.

When customers make large cash transactions, such as over $10,000, a currency transaction report (CTR) needs to be filed with the government that includes customer information. The bank would need to evaluate if this cash transaction is in accord with the customer's expected legitimate banking activity. When customers behave suspiciously, or in a manner to indicate criminal activity, the bank has a duty to investigate, and report this suspicious activity to FinCEN as a suspicious activity report (SAR).

For example, suppose a customer tells the bank he is unemployed, yet he regularly deposits large amounts of cash into his account. The bank would be required to investigate this, and probably report it via a SAR. If the customer deposits $9,999 in cash on two separate days, that might not require the filing of a CTR, but it might require the filing of a SAR, because the customer appears to be structuring deposits to try avoid having a CTR filed. If the customer states that he is involved with selling merchandise on eBay, but deposits large volumes of cash, or receives high dollar bank wires, that would be worthy of further investigation. If a customer is a victim of a fraud, or is a participant in a fraud, the bank's AML personnel need to investigate, and probably file a SAR.

All of these CTRs and SARs go to FinCEN and are accessible to certain law enforcement throughout the country. As indicated previously, the information filed with FinCEN is secret, and unauthorized disclosure is a serious criminal offense. Government and bank employees are not allowed to disclose their filings, nor even the fact that a filing was made. Thus, while it is well known that SARs need to be filed, it is a crime to disclose the filing of a particular SAR. Thus it would be improper to ask someone to disclose this information.

Money Laundering Typologies and Examples

The money laundering investigator should be aware of various typologies, some of which are summarized here, keeping in mind that the criminal's creativity is unbounded by existing frameworks. After all, typologies are merely criminal conduct that has been discovered and written about. Imagine the criminal conduct that has not yet been identified.

Typologies

Structuring is the process of breaking up one payment into smaller, less-recognized payments to avoid reporting requirements. (31 U.S.C. § 5324, Dept. Treasury National Money Laundering Risk Assessment 2015, ACAMS Study Guide p. 20). If the drug dealer desires to deposit $50,000 in cash into the bank, he might chose to do that $5,000 per week, for 10 weeks, thus structuring the deposits to avoid reporting requirements.

Smurfing is similar to structuring, but it involves using many people to disguise the transaction (FATF Report on Money Laundering Typologies 1998, ACAMS Study Guide p. 20). If the drug dealer desires to deposit $50,000 in cash to a bank, he could give $5,000 to ten of his employees or associates, who deposit it into their own bank account. Then they each make a payment to the drug dealer by check or wire.

Bulk cash smuggling is used to avoid cash reporting requirements at the border. (31 U.S.C. § 5332, Dept. Treasury National Money Laundering Risk Assessment 2015, p. 27, ACAMS Study Guide). The USA requires individuals transporting over $10,000 across the border to report this, but criminals cannot declare their cash, so it is hidden on their person, in their luggage, or in the vehicle. Drug traffickers who smuggle drugs into a country may use similar techniques to smuggle cash profits out of the country.

Trade-based money laundering uses the ruse of an international transaction to transfer value secretly from one place to another (Dept. Treasury National Money Laundering Risk Assessment 2015, p. 29, ACAMS Study Guide p. 55). This can be done through fictitious invoicing, over-invoicing, and under-invoicing. With a fictitious invoice, Company A provides an invoice to Company B, but no goods or services were really provided. Company A receives payment from Company B, and the funds appear legitimate. With over- or under-invoicing, Company A provides goods or services to Company B, but the invoice is either much higher or lower than the value provided. When Company B pays Company A, net value is transferred but the amount and direction of transfer is disguised.

Shell companies disguise the true ownership and control of the company (Dept. Treasury National Money Laundering Risk Assessment 2015, ACAMS Study Guide). The criminal uses a shell corporation, ABC Corp, so that the account is not in his true name. It is hard to identify the owners and directors of ABC Corp, because it, in turn, is owned by XYZ Corp. Where incorporation documents were filed with the government, they were filed by a business that protects the confidentiality of its clients. Shell corporations may be incorporated on one country, but use bank accounts in another country, picking countries that provide confidentiality. *Front companies* are a variation on this theme, where an ostensibly legitimate business is merely a disguise for money laundering or other nefarious activity.

Salaries can be used to launder funds (ACAMS Study Guide p. 70). A criminal may be on the payroll of a company and is paid a salary as if he works there, but in fact does not. Or, companies might pay employees in cash derived from criminal proceeds.

Attorneys and accountants may be used by money launderers, wittingly or not, to launder funds (Dept. Treasury National Money Laundering Risk Assessment 2015, ACAMS Study Guide p. 148). A tiny percentage of these professionals use their expertise unlawfully by actively assisting criminals with the commission of crimes such as money laundering and tax evasion, by giving advice on how to commit crimes and escape detection. Some may inadvertently provide services that assist criminals with shielding assets or transactions from government view. Of course, the vast majority of attorneys and accountants are honest, giving ethical advice to law abiding clients including about how to comply with laws and regulations.

Real estate can be used as a vehicle for money laundering (Dept. Treasury National Money Laundering Risk Assessment 2015, ACAMS Study Guide). Where funds are sent or received from shell companies, property is owned by a shell company, or attorneys are used to send or

receive funds on behalf of the client; there is the ability to disguise the true ownership, source, or destination of funds.

Cybercrime has created new money laundering typologies (Dept. Treasury National Money Laundering Risk Assessment 2015, Bandler, Stemming the Flow of Cybercrime Payments, ACAMS TODAY, June 9, 2017). Cybercrime is conducted through the internet, making cash an inconvenient payment mechanism. Virtual currencies (e.g. Egold, Liberty Reserve, or Bitcoin) have become a payment method of choice between criminal participants. Cybercrime is tied to identity theft and also involves theft of funds in a variety of formats, including through bank wire, forged checks, and credit or debit accounts.

Money mules are recruited by cybercriminals to move money on their behalf (Dept. Treasury National Money Laundering Risk Assessment 2015, Bandler, Stemming the Flow of Cybercrime Payments, ACAMS TODAY, June 9, 2017). These money mules, wittingly or not, receive forged checks and misdirected bank wires, and send the funds to the next destination on behalf of criminals. Cybercriminals are constantly recruiting these money mules, through work-at-home scams, romance scams, or sophisticated schemes that purportedly involve collecting a debt or otherwise receiving a payment.

Traditional business can be created or coopted for the purpose of receiving criminal proceeds, for making payments which appear to be legitimate, and which can even be reported on taxes (Dept. Treasury National Money Laundering Risk Assessment 2015). Suppose the drug kingpin earns over a million dollars in cash per year – more cash than he can use or store himself. He reaches an agreement with a restaurant owner, and he gives the restaurant owner $20,000 in cash every month. The restaurant owner makes regular bank deposits for the day's cash receipts and includes a portion of the drug dealer's cash with each deposit. The bank and tax authorities are told this is restaurant income, though it is mostly drug dealing income. The restaurant's bank balance swells each month, and the drug dealer receives a monthly check for $10,000 under the guise he is a part owner, a salaried employee, or a vendor of supplies or services to the restaurant. Ultimately, the drug dealer might want to launder more funds, so he could buy – or create – businesses to use as front companies to do this.

Investigation Considerations

The money laundering investigator should consider how the criminal profits are earned, how criminals pay each other, do business, and reap the benefits. In other words, think like the criminal. The investigator should not only "follow the money" but also "follow the product," because this will give insight about where the money is going. Monetary transactions accompany transfer of contraband and criminal services (Bandler, Lawyers, Drugs and Money, AML in Popular Media 2018). After all, criminals do not provide goods or services for free, they are doing it to get paid. For example, suppose drugs are grown and manufactured in South America, and delivered to various cities in the United States, and then sold on the streets for cash. The drugs follow a path through farming, processing, shipment, repackaging, and sale, and many people play a role at each stage of this process. The drug "kingpins" within the United States and South America are reaping significant profits, and beneath them are a wide spectrum of employees, workers, and contractors, some of whom earn handsomely while others earn a pittance. The sale of the drugs on the street is done for cash, the street dealer and team are paid, give cash to their boss, and so on up the chain. Much of that profit needs to ultimately make its way back to the country of drug origin to pay the kingpin, traffickers, and laborers. Perhaps cash is smuggled to South America, or perhaps funds are sent via bank wire of virtual currency. Funds need to be transferred in a manner that is cost efficient, safe, and hidden from government detection.

Cybercrime Money Laundering

Cybercrime has altered the traditional money laundering models, since illicit profits are often earned in virtual currency rather than cash, presenting different money laundering challenges for

the criminal, and a different typology for law enforcement, regulators, and private investigators (Bandler, Stemming the Flow of Cybercrime Payments 2017). Law enforcement is still learning how to effectively address cybercrime and how it launders funds. Here is an example of cybercrime money laundering: A hacker from another country hacks into a US-based company and steals millions of records, such as credit card account information, credit report information, internet usernames and passwords, or other victim information. The hacker sells this information to a "vendor" of stolen data, who pays for the data in virtual currency. Next, the vendor sells this hacked data to identity thieves in the USA, who also pay with virtual currency. The identity thieves work with their associates to commit identity theft, to create forged identification and credit cards, to assume the identity of the victims, use their credit to purchase merchandise or otherwise steal. These participants never meet each other, never learn each other's true name, but still need to pay each other. Cash is of little use, but virtual currency works perfectly. The cybercriminals earn prodigious profits in virtual currency and need to launder those funds.

Prosecution Examples

Since the creation of money laundering criminal laws, there have been many prosecutions of those who hid their own illegal profits, as well as those who facilitated their activity. Financial institutions can be held liable both criminally and civilly for their customers' activity. In the early 1990s, it was discovered that the Bank of Credit and Commerce International (BCCI) was involved with massive money laundering and fraud and were charged federally in Florida and with state charges by the New York County District Attorney's Office. BCCI ultimately pleaded guilty in state and federal court and forfeited over a half a billion dollars and went out of business. In 2014, BNP Paribas pleaded guilty to falsifying business records in a scheme to illegally move funds on behalf of sanctioned individuals and entities, and paid nearly nine billion dollars in penalties but remained in operation. In 2012, HSBC entered into a deferred prosecution agreement with state and federal authorities and paid nearly two billion dollars in fines for falsifying records, laundering funds on behalf of drug traffickers, and transmitting funds for sanctioned entities. Other banks have been fined by federal and state regulators for falling short with their AML requirements.

As mentioned, cybercrime launched a new era in crime and money laundering, including through virtual currency. Egold was the first virtual currency, invented in the mid-1990s, and became popular with cybercriminals and identity thieves. In 2007, Egold was charged by federal authorities of money laundering and illegal money transmitting and was convicted by guilty plea in 2008.

Western Express International, Inc. was a virtual currency exchanger based in Manhattan which facilitated cybercrime and identity theft related conduct, and laundered funds for its customers. In an investigation that spanned from 2005 to 2013, the New York County District Attorney's Office investigated the exchanger, followed the money (digital currency), and ultimately identified many of the exchanger's clients. Cybercriminals were extradited from Eastern Europe, identity thieves were arrested across the USA, and the exchanger and its owners were also charged. Most defendants admitted their responsibility through guilty plea, and the remaining three were convicted after a trial that lasted over 2 months. This case provided a window into the global nature of cybercrime, virtual currency, and money laundering techniques through digital currency, money remittances, bank wires, and shell corporations.

Liberty Reserve was a virtual currency based in Costa Rica, which also catered to criminal conduct by cybercriminals, identity thieves, and others. In May 2013 the business and owners were indicted by federal authorities, and they were ultimately convicted by guilty plea of money laundering. The prosecution of Silk Road mastermind Ross Ulbricht marked another successful cybercrime money laundering case. Ulbricht had created and operated an online marketplace for drugs and other contraband, where participants paid each other with Bitcoin virtual currency. The public is interested in crime stories,

so money laundering investigation has found its way into television and movies, including the television series The Wire, Breaking Bad, Ozark, and more (Bandler, Lawyers, Drugs and Money, AML in Popular Media, March 20, 2018).

Anti-Money Laundering Organizations

There are a number of organizations that address or focus on anti-money laundering issues, including international, governmental, non-profit, and for-profit trade organizations. Every country's financial intelligence agency (e.g., FinCEN) can join with the international Egmont Group of Financial Intelligence Units, which promotes cross-border cooperation with financial investigations. The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental organization devoted to combating money laundering, terrorist financing, and other threats to the international financial system. The United Nations has devoted resources toward anti-money laundering, established the Office on Drugs and Crime, and offers model legislation that countries may choose to adopt. The Association of Certified Anti-Money Laundering Specialists (ACAMS) is the largest international membership organization dedicated to anti-money laundering and administers a professional certification. There are also other professional organizations for AML professionals. Other organizations and resources are listed in the additional reading section.

Conclusion

Money laundering investigation is conducted by many participants from the government, financial, private, legal, and journalism sectors. Through proper investigative techniques, criminal activity and profits can be identified and minimized. Legal and regulatory requirements may impose a duty to adequately detect and investigate money laundering activity.

Cross-References

- ▶ Criminals: Cybercriminals
- ▶ Criminals: Terrorists
- ▶ Criminals: White-Collar Crimes
- ▶ Internet (Deep and Dark Web)
- ▶ Investigations: Bank Fraud
- ▶ Investigations: Criminal
- ▶ Investigations: Employee Theft of Employer Property
- ▶ Investigations: Fraud
- ▶ Investigations: Terrorism
- ▶ Law: Administrative

References

ACAMS Study Guide for the Certified Anti Money Laundering Specialist (CAMS) Certification Exam. (2016). ACAMS, 6th ed., p. 65.

All the President's Men. (1976). Wildwood enterprises/ Warner bros.

Bandler, J. (2016). Cybercrime and digital currency, p. 9, *Information Law Journal, A Publication of the Information Security and EDDE Committees, ABA Section of Science & Technology Law, 7* (4), Autumn. https://www.americanbar.org/content/dam/aba/administrative/science_technology/2016/ilj_volume7_issue4.authcheckdam.pdf

Bandler, J, Lawyers Drugs, and Money, AML in Popular Media, ACAMS TODAY, 20 Mar 2018. https://www.acamstoday.org/lawyers-drugs-and-money-aml-in-popular-media/

Bandler, J. Stemming the flow of cybercrime payments, ACAMS TODAY, 9 June 2017. https://www.acamstoday.org/stemming-the-flow-of-cybercrime-payments/

CFPB (Consumer Financial Protection Bureau). https://www.consumerfinance.gov/about-us/. Last accessed 26 Apr 2018.

Department of the Treasury. (2015). National Money Laundering Risk Assessment, 2015). https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

FATF (Financial Action Task Force) Report on money laundering typologies, 1998.

FDIC (Federal Deposit Insurance Corporation). https://www.fdic.gov/about/strategic/strategic/mission.html. Last accessed 26 Apr 2018.

FinCEN, (U.S. Department of the Treasury, Financial Crimes Enforcement Network) (FinCEN). https://www.fincen.gov/about/mission. Last accessed 26 Apr 2018.

OECD. (2016). *Illicit trade: Converging criminal networks, OECD reviews of risk management policies*

(p. 15). Paris: OECD. https://doi.org/10.1787/9789264251847-en.
UNODC (United Nations Office on Drugs and Crime) website. The Money-Laundering Cycle. https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html. Last visited 26 Apr 2018.

Further Reading

Government Related

Egmont Group of Financial Intelligence Units. https://egmontgroup.org/en
Financial Action Task Force on Money Laundering (FATF). http://www.fatf-gafi.org
U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC). https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx
U.S. Department of the Treasury. Financial Crimes Enforcement Network (FinCEN). https://www.fincen.gov
U.S. Federal Financial Institutions Examination Council (FFIEC). Bank Secrecy Act/Anti-Money Laundering Information Base, http://www.ffiec.gov/bsa_aml_infobase/default.htm
United Nations Office on Drugs and Crime. http://www.unodc.org

Professional Organizations

American Bankers Association. https://www.aba.com
Association of Certified Anti-Money Laundering Specialists (ACAMS). http://www.acams.org
Florida International Bankers Association (FIBA). http://www.fiba.net
International Money Laundering Information Network. http://www.imolin.org/imolin/en
The Anti-Money Laundering Association (AMLA). https://theamla.com
Wolfsberg Group. www.wolfsberg-principles.com

Journalist and Non-profit AML Investigation

Global Witness. https://www.globalwitness.org
International consortium of investigative journalists. https://www.icij.org/
Organized Crime and Corruption Reporting Project. https://www.occrp.org

Statutes

USA PATRIOT Act. For a summary see https://www.justice.gov/archive/ll/highlights.htm
31 U.S.C. §5311 *et seq*. Bank Secrecy Act (BSA).
18 U.S.C. § 1956 Laundering of monetary instruments.
18 U.S.C. § 1957 Engaging in monetary transactions in property derived from specified unlawful activity.
18 U.S.C. § 1960 Unlicensed money transmitting.
31 U.S.C. § 5330 Registration of money transmitting businesses.
NYS Penal Law § 470.00 *et seq*., Money laundering.
NYS Banking Law § 650, Unlicensed money transmitting.

AML News Sites, Guides, and Articles

ACAMS MoneyLaundering.com. www.moneylaundering.com
ACAMS Study Guide for the Certified Anti Money Laundering Specialist (CAMS) Certification Exam. (2016). ACAMS, 6th ed.
Bandler, J. Cybercrime and digital currency. *ABA Information Law Journal* (Autumn 2016). https://www.americanbar.org/content/dam/aba/administrative/science_technology/2016/ilj_volume7_issue4.authcheckdam.pdf
Bandler, J. Dirty digital dollars, Fraud Magazine (July/August 2016). http://www.fraud-magazine.com/article.aspx?id=4294993652
Bandler, J. (2017). Stemming the flow of cybercrime payments and money laundering. ACAMS TODAY, 16 (3). http://www.acamstoday.org/stemming-the-flow-of-cybercrime-payments/
Money Laundering Bulletin. https://www.moneylaunderingbulletin.com

Investigations: Negligence

Thomas Shea
Police Graduate Studies Program, College of Education and Human Services, South Orange, NJ, USA

Keywords
Investigation · Negligence · False confessions · Exclusionary rule · Wrongful convictions · Entrapment · Failure to train · Failure to supervise

Definition

This entry focuses more on a singular form of occupational obligation failure, that is, investigation negligence. These failures occur because of various reasons, including the following: neglect of duty, oversight, incompetence, and recklessness. Investigation negligence has the potential

to affect court dispositions, incarcerate the innocent, and cause unnecessary stress and trauma to already suffering crime victims. Additionally, there remains a causal and replicated link between investigation negligence and costly litigation expenses incurred by police departments in the United States. Training and proper supervision are employed to mitigate the adverse effects of investigation negligence, yet a prevalence still occurs.

Introduction

Negligence is defined as, "a failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances. The behavior usually consists of actions, but can also consist of omissions when there is some duty to act (e.g., a duty to help victims of one's previous conduct) (http://www.law.cornell.edu)." All behavior based on forecasts instead of results creates some level of potential harm, causing risk (Gilles 2000). Negligence, on the other hand, is unjustifiable risk, or actions that a reasonable person would not undertake given the same circumstances (Model Penal Code 2.02(2)(d)). When risks are unjustifiable and the justifications for taking them are minimal, negligence become "gross" (Moore and Hurd 2011). Investigation negligence presents during various aspects of investigation, but those affected as a result have the propensity to be detrimental.

According to Rossmo (2009), there are three primary causes leading to the investigative failures due to negligence: cognitive biases, organizational traps, and probability errors. Cognitive biases include memory limitations that lead mental errors due to the simplification of information processing (Heuer 1999). The memory of an average human being only holds a certain amount of information, ultimately leading to a false supporting of our hypotheses (Schacter 2001). Organizational traps include rumors and ego, among other aspects (Rossmo 2009). Rumors and misinformation negatively impacts the trajectory of investigations, leading to many well-known cases to venture down erroneous directions (Campbell 1996). Ego often causes the failure of an investigator to adapt to the acquisition of new, dissenting information (Rossmo 2009). Differing word meanings vary between the message sender and the receivers (Heuer 1999). Probability errors in judgment and decision making are often the result.

Investigative Mistakes

Discounting of pertinent information is precipitated by behavior such as anchoring, selective perception, and "onus probandi," transference of the burden of proof to the suspect instead of the investigator (Ditrich 2015). While not permissible in a court setting, there are plenty of opportunities to occur in the investigative field. Anchoring involves the overestimation of uncorroborated, partial evidence; even when new evidence disputes its legitimacy. Validation of inconsistent evidence undermines accuracy because evidence that challenges chosen hypotheses is disregarded (O'Brien 2009). Subsequently, "attractive" subjects may emerge from the formation of biased opinions of investigators, who consider high the likelihood that they committed the crimes investigated (Saladin et al. 1988). Judgments concerning the accountability of certain suspects are thus stronger as a result (Sigall and Ostrove 1975), whether correct or not. "Innocent until proven guilty" is a fundamental, Constitutional right in the United States; yet, both inter- and intraorganizational pressures may compel investigators to solve cases hastily, thus causing the aforementioned mistakes (Krix and Sauerland 2011).

Results of Investigative Negligence

False Confessions

Negligent investigation can result in false confessions, causing the true perpetrator to remain unapprehended and free to commit additional crimes (Doyle 2010; Russano 2004). Although more attention has been recently focused on this issue, the fact remains that a

large number of criminal convictions are the outcome of false confessions (Dwyer et al. 2000; Kassin and Neumann 1997; Rattner 1988). Kassin and Wrightsman (1985) identified three types of false confessions: (a) coerced compliant false confessions, (b) voluntary false confessions, and (c) coerced-internalized false confessions. Other researchers (Kassin and Gudjonsson 2004) examined a large amount of data including case studies, field experiments and correlational reports. They concluded that police interrogation tactics will likely continue producing false confessions.

False Witness Statements

Many false confessions are the byproduct of incorrect or false statements from witnesses; in fact, three quarters of hundreds of subsequent false confessions originated from false witness statements (Garrett 2011). The revelation of this dilemma led to a resurgence of the use of expert witnesses by defense attorneys in court, to refute the reliability of false statements (Loftus 2013). Newring and O'Donohue (2008) conducted a study resulting in findings implicating the fact that police are following investigative leads based on false statements, some of them unintentionally.

Entrapment

Under a legal entrapment defense, an individual may not be convicted of a criminal offense if encouraged by the government to do so in certain circumstances (Dillof 2003). Criminal defense attorneys utilize this type of defense often during narcotics cases. The fact-finder must determine and conclude that absent the aforementioned encouragement by government intervention, the defendant would not have committed the criminal act (Allen 1999). As a general rule in legal proceedings, this defense is unavailable if the actor created any conditions that established self-imposed culpability (Robinson 1985).

Forensic Negligence

One of the most significant forensic science scandals occurred at the Houston Police Department Crime Laboratory in 2002. After a formation of an investigative team, forensic analyses reviewed 3500 past cases conducted by scientists at that agency. The investigation culminated in a report detailing numerous, negligent errors committed by staff, even in death penalty cases (Bromwich 2007). State-level oversight likely could have prevented this scandal, at least not allowing it to deteriorating to such a vast level (Goldstein 2011).

Fingerprinting forensic science is not immune to false positive either. Fundamental decisions made by fingerprint experts are prone to contextual influences, leading to errors (Dror et al. 2006). Independent objectivity in the processing and evaluation of information are limited due to cognitive flaws (Dror et al. 2005).

Causal Effect of Investigative Negligence: Failure to Train

The United States Supreme Court case Canton v. Harris (1989) held that the failure to train police officers or investigators exposes police departments to organizational liability, under Title 42 United States Code Section 1983. Deficient training rises to a liable level when a petitioner confirms to the Court that the failure to train by the police department amounts to "deliberate indifference." This concept means that the training deficiencies were negligent enough to significantly raise the level of risk to others they may come into contact with (Ross 2000). Deliberate indifference, as stated in Farmer v. Brennan (1994), consists of a pattern amid "mere negligence and something less than acts or omissions for the very purpose of causing harm or with knowledge that harm will result (Vaughn et al. 2001)." The Court must decide when that balance tips towards indefensible negligence. The two most common forms of claims of this form against police administrators usually fall under allegation of failing to train and failing to supervise (Kappeler 1997; Barrineau 1994).

Protection from Investigation Negligence: The Exclusionary Rule

Before discussing the exclusionary rule, there exists an importance to understand the concept of "evidence laundering (Levine et al. 2016)." This action occurs when officers or investigators make Constitutional mistakes while gathering evidence. Ultimately, that same evidence is transferred to others in their respective agencies, then to prosecutors to make a case. The original mistake, the exposure of which should taint the rest of the evidence in a criminal case, remains hidden. If that evidence is not only negligently gathered but also passed along to a second officer, negligence presents at both the investigator and supervisory levels. The holding in US v. Leon allows for "good faith" exceptions to the exclusionary rule, where criminal evidence illegally obtained would otherwise subjected to suppression. This decision essentially allows for investigative negligence to occur in some respects, unless the negligence rises to the "deliberate indifference" level. Concern arises, however, when there is no knowledge of the original violation. The Courts determined that outlawing single, illegal acts does not deter police conduct. Eliminating the systemic disregarding of Constitutional standards is the objective of the exclusionary rule (Herring v. U.S.). This approach appears to repudiate negligence as a primary factor that would trigger the exclusionary rule, asunder the assumption that reckless behavior can be deterred more readily (Bradley 2012). Courts mandate that prosecutors turn overall items of evidentiary value to the defense, even those that undermine the State's case (Brady v. Maryland; Jones 2010). The problem is awareness of that evidence must exist to the Court in the first place.

The Price of Investigative Negligence: Wrongful Convictions

The price to government officials for investigative negligence is the loss of a conviction and possibly professional embarrassment. The price for defendants is unconstitutional loss of freedom. In 1989, four youths were arrested for the brutal sexual assault and beating of a jogger in New York City's Central Park. The boys all asserted their innocence (Bickel 2002) yet were convicted after a trial and sentenced to prison. An individual identified as Matias Reyes later admitted to the crime, exonerating the defendants (Russano 2004). Nobles and Schiff (2000) contend that operational negligence in policing is routine and are skeptical of the potential that there are authentic reforms in place. The striving of investigators and prosecutors to build the case against an identified accused party tends to increase the acceptance of errors and negligence (Huff et al. 1996). Scheck et al. (2001) reviewed 74 cases of individuals who were freed from prison, due to the efforts by The Innocence Project, an organization that utilizes DNA analysis to exonerate the wrongfully convicted. Some of the more prominent reasons causing the eventual miscarriages of justice included: mistaken identification (82%), police misconduct (50%), trial misconduct (45%), defective forensic science poor defense lawyers (32%), false confessions (witness testimony (20%). The University of California-Irvine and the University of Michigan Law School together formed an organization titled the National Registry of Exonerations (www.law.umich.edu). Compiled statistics for the year 2018 were as follows: There were 151 exonerations. 68 individuals were exonerated of homicide, 17 for sexual crimes, 16 for violent crimes, and 47 for nonviolent crimes. Official misconduct by police officials was the primary characteristic in 107 of the cases, including 54 of the homicide case (79%) exonerations. The state with the most exoneration was Illinois with 49 of the cases, with the next state being New York with 16, demonstrating a prevalent culture of police negligence. Prisoners lost a combined 20,000 years of freedom to false imprisonment. Eighteen years spanned the two studies, and wrongful convictions continue to occur in high numbers, indicating that not enough reform occurred in that time.

Conclusion

Whether an officer on street patrol or an investigator working homicide case, the propensity for negligence is always present. As we have seen in this literature, even if there are competent supervisors capable of recognizing and correcting negligent errors, the possibility remains that they are sometimes not aware in the first place to act. Police officers have a vast amount of discretion while performing their duties during investigations. Without a credible checks and balances system implemented as the norm, human error may persist undetected. As a result, violations of citizens' Constitutional rights will likely continue. As the efforts of the Innocence Project continue to prove, innocent defendants will also continue to be sent to prison for crimes they did not commit. A secondary issue emerges in the courts, where a "minor" act of negligence is not necessarily considered enough to suppress evidence unless it rises to a level of "deliberate indifference." The "good faith" exception to the exclusionary rule, as legal scholars in this chapter indicated, appears to carve out rationalization for negligence. While it is unknown whether the Court will revisit this issue in the future is uncertain. What is certain is the likelihood that human fallibility will continue to produce negligent errors during investigations. While society does not purport to tolerate negligence in the criminal justice system, there also does not seem to be a strategy in place to stem future occurrences. The Innocence Project has made great strides in exposing negligence and exonerating the innocent, yet DNA analysis is not immune to human negligence anymore than fingerprint analysis. More extensive training for investigative supervisors could inhibit the prevalence of occurrences, along with more stringent legal inquiries regarding criminal evidence.

Cross-References

► Investigations: Criminal

References

Allen, R. (1999). Clarifying entrapment. *Journal of Criminal Law and Criminology, 89*, 407.

Barrineau, H. E. (1994). *Civil liability in criminal justice* (2nd ed.). Cincinnati: Anderson Publishing Company.

Bickel, B. (2002). The Central Park jogger. Retrieved from http://crirne.about.com/library/bifiIes/bl-cpj.htm

Bradley, C. M. (2012). Is the exclusionary rule dead? *The Journal of Criminal Law and Criminology, 102*(1), 1–23.

Bromwich, M. (2007). *Final report of the independent investigator for the Houston police department crime laboratory and property room 54–57*. Retrieved from: http://www.hpdlabinvestigation.org/reports/070613report.pdf

Campbell, J. A. (1996). *Bernardo investigation review*. Toronto: Government of Ontario.

City of Canton, Ohio v. Harris, 489 U.S. 378 (1989)

Clipper v. Takoma Park, 876 F.2d 18 (4th Cir. 1989).

Dillof, A. M. (2003). Unraveling unlawful entrapment. *The Journal of Criminal Law and Criminology, 94*, 827.

Ditrich, H. (2015). Cognitive fallacies and criminal investigations. *Science & Justice, 55*(2), 155–159.

Doyle, J. M. (2010). Learning from error in American criminal justice. *The Journal of Criminal Law and Criminology, 100*, 109. https://doi.org/10.2307/20753686.

Dror, I. E., Peron, A., Hind, S., & Charlton, D. (2005). When emotions get the better of us: The effect of contextual top-down processing on matching fingerprints. *Applied Cognitive Psychology, 19*(6), 788–809.

Dror, I. E., Charlton, D., & Peron, A. E. (2006). Contextual information renders experts vulnerable to making erroneous identifications. *Forensic Science International, 156*(1), 74–78.

Dwyer, J., Neufield, P. J., & Scheck, B. (2000). *Actual innocence: Five days to execution and other dispatches from the wrongly convicted*. New York: Doubleday Books.

Farmer v. Brennan, 511 U.S. 825 (1994)

Garrett, B. L. (2011). *Convicting the innocent*. Cambridge, MA: Harvard University Press.

Gilles, D. (2000). *Philosophical theories of probability*. London: Routledge.

Goldstein, R. M. (2011). Improving forensic science through state oversight. *Texas Law Review, 90*, 225.

Herring v. United States, 555 135 (2009).

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Washington, DC: Center for the study of Intelligence, Central Intelligence Agency.

http://www.law.umich.edu/special/exoneration/Pages/about.aspx

Huff, R., Rattner, A., & Sagarin, E. (1996). *Convicted but innocent: Wrongful conviction and public policy*. Thousand Oaks: Sage.

Jones, C. (2010). A reason to doubt: The suppression of evidence and the inference of innocence. *The Journal of Criminal Law and Criminology, 100*(2), 415–474.

Kappeler, V. E. (1997). *Critical issues in police civil liability* (2nd ed.). Prospect Heights: Waveland Press.
Kassin, S. M., & Neumann, K. (1997). On the power of confession evidence: An experimental test of the fundamental difference hypothesis. *Law and Human Behavior, 21*, 469–484. https://doi.org/10.1023/A:1024871622490.
Kassin, S. M., & Gudjonsson, G. H. (2004). The Psychology of Confessions: A Review of the Literature and Issues. *Psychological Science in the Public Interest, 5*(2), 33–67. https://doi.org/10.1111/j.1529-1006.2004.00016.x
Kassin, S. M., & Wrightsman, L. S. (1985). Confession evidence. In S. Kassin & L. Wrightsman (Eds.), *The psychology of evidence and trial procedure* (pp. 67–94). Beverly Hills: Sage.
Krix, A. C., & Sauerland, M. (2011). About sources of error of testimonies. *Inquisitive Mind, 1*, 12–21.
Levine, K. L., Turner, J. I., & Wright, R. F. (2016). Evidence laundering in a post-herring world. *The Journal of Criminal Law and Criminology, 106*, 627.
Loftus, E. F. (2013). 25 years of eyewitness science. . . . .Finally pays off. *Perspectives on Psychological Science, 8*(5), 556–557. https://doi.org/10.1177/1745691613500995.
Model Penal Code 2.02(2)(d).
Moore, M. S., & Hurd, H. M. (2011). Punishing the awkward, the stupid, the weak, and the selfish: The culpability of negligence. *Criminal Law and Philosophy, 5*, 147–198. https://doi.org/10.1007/s11572-011-9114-0.
Newring, K. A., & O'Donohue, W. (2008). False confessions and influenced witnesses. *Applied Psychology in Criminal Justice, 4*(1), 81–107.
Nobles, R., & Schiff, D. (2000). *Understanding miscarriages law, the media, and the inevitability of crisis*. Oxford: Oxford University Press.
O'Brien, B. (2009). An examination of factors that aggravate and counteract confirmation bias in criminal investigations. *Psychology, Public Policy and Law, 15*(4), 315–334.
Rattner, A. (1988). Convicted but innocent: Wrongful conviction and the criminal justice system. *Law and Human Behavior, 12*, 283–293.
Robinson, P. (1985). Causing the conditions of one's own defense: A study in the limits of theory in criminal law doctrine. *Virginia Law Review, 71*, 1.
Ross, D. L. (2000). Emerging trends in police failure to train liability. *Policing: An International Journal of Police Strategies & Management, 23*(2), 169–193.
Rossmo, D. K. (2009). *Criminal Investigative Failures*. Taylor & Francis. Boca Raton, FL.
Russano, M. B. (2004). *True and false confessions to an intentional act: A novel experimental paradigm* (Doctoral dissertation). Retrieved from https://digitalcommons.fiu.edu/dissertations/AAI3128613
Saladin, M., Saper, Z., & Breen, L. (1988). Perceived attractiveness and attributions of criminality: What is beautiful is not criminal. *Canada Journal of Criminology, 30*, 251–259.
Schacter, D. L. (2001). *The seven sins of memory: How the mind forgets and remembers*. Boston: Houghton Mifflin.
Scheck, B., Neufeld, P., & Dwyer, J. (2001). *Actual innocence: When justice goes wrong and how to make it right*. New York: Signet.
Sigall, H., & Ostrove, N. (1975). Beautiful but dangerous: Effects of offender attractiveness and nature of the crime on jurisdictional judgment. *Journal of Personality and Social Psychology, 31*, 410–414.
United States v. Armstrong, 517 U.S. 456 (1996).
United States v. Leon, 468 897 (1984).
United States v. Woerner, 709 533–35 (F3d 527 2013).
Vaughn, M. S., Cooper, T. W., & del Carmen, R. V. (2001). Assessing legal liabilities in law enforcement: Police chiefs' views. *Crime and Delinquency, 47*(1), 3–27. https://doi.org/10.1177/0011128701047001001.

Investigations: OSHA

Rifath Ali and Troy Rawlins
Department of Safety, Security, and Emergency Management, College of Safety and Justice, Eastern Kentucky University, Richmond, KY, USA

Keywords
OSHA · OSH Act · General Duty Clause · Regulations · Guidelines · Rules · Ergonomics · Musculoskeletal Disorders · MSDs · General industry · Construction industry · Maritime industry · Agriculture industry · NIOSH · Crystalline Silica · Silicosis · Silica dust

Definition

OSHA – With the Occupational Safety and Health Act of 1970, Congress created the Occupational Safety and Health Administration (OSHA) to ensure safe and healthful working conditions for working men and women by setting and enforcing standards and by providing training, outreach, education, and assistance (OSHA-About n.d.).

Introduction

In 1970, the US Congress passed the Occupational Safety and Health Act (OSH Act). Subsequently, following the passage of Public Law 91-596 in April 1971, the Occupational Safety and Health Administration was established within the federal Department of Labor (DOL). Commonly called The OSHA Act, this legislation was signed into law by President Richard Nixon. The Act was created to establish uniform governmental safety and health standards and regulations to achieve two primary congressional purposes: (1) protect American workers from safety and health hazards in their work environments and (2) protect employers from the burden of costs associated with workplace injuries and illnesses while protecting interstate commerce and production. OSHA did not develop all new standards and regulations for safety and health unilaterally, but rather, adopted by reference many existing industry-specific regulations, such as those found within National Electric Code (NEC), American Congress of Industrial Hygienist (ACGIH), National Fire Protection Association (NFPA), and the Compressed Gas Association (CGA), and codified them within title 29 of the Code of Federal Regulations (CFR). The Act mandates that companies have a "responsibility or duty" to retain a work environment without identified hazards. The Act also tasked OSHA specifically with 13 targeted objectives to ensure both voluntary and involuntary employer compliance with standards and regulations set by the US Congress. According to OSHA's website, www.OSHA.gov, these objectives include:

(1) Encouraging employers and employees in their efforts to reduce the number of occupational safety and health hazards at their places of employment, and to stimulate employers and employees to institute new and to perfect existing programs for providing safe and healthful working conditions;
(2) Ensuring that employers and employees have separate but dependent responsibilities and rights with respect to achieving safe and healthy working conditions;
(3) Authorizing the Secretary of Labor to set mandatory occupational safety and health standards applicable to businesses affecting interstate commerce, and by creating an Occupational Safety and Health Review Commission for carrying out adjudicatory functions under the Act;
(4) Building upon advances already made through employer and employee initiative for providing safe and healthful working conditions;
(5) Providing for research in the field of occupational safety and health, including the psychological factors involved, and by developing innovative methods, techniques, and approaches for dealing with occupational safety and health problems;
(6) Exploring ways to discover latent diseases, establishing causal connections between diseases and work in environmental conditions, and conducting other research relating to health problems, in recognition of the fact that occupational health standards present challenges often different from those involved in occupational safety;
(7) Providing medical criteria, which will assure insofar as practicable that no employee will suffer diminished health, functional capacity, or life expectancy as a result of his work experience;
(8) Providing for training programs to increase the number and competence of personnel engaged in the field of occupational safety and health, affecting the OSH Act since its passage in 1970 through January 1, 2004.
(9) Providing for the development and promulgation of occupational safety and health standards;
(10) Providing an effective enforcement program which shall include a prohibition against giving advance notice of any inspection and sanctions for any individual violating this prohibition;
(11) Encouraging the States to assume the fullest responsibility for the administration and enforcement of their occupational safety and health laws by providing grants to the States to assist in identifying their needs and responsibilities in the area of occupational safety and health, to develop plans in accordance with the provisions of this Act, to improve the administration and enforcement of State occupational safety and health laws, and to conduct experimental and demonstration projects in connection therewith;
(12) Providing for appropriate reporting procedures with respect to occupational safety and health, which will help achieve the objectives of this Act and accurately describe the nature of the occupational safety and health problem;

I

(13) and lastly, encouraging joint labor-management efforts to reduce injuries and disease arising out of employment. (www.OSHA.gov 2019)

Upon the creation of the OSHA Act, the US Congress recognized a need for a special provision within the Act that is called the *General Duty Clause.* The General Duty Clause is *also* commonly referred to as a *5(a)(1). It* is a "catch-all" designed for OSHA to address workplace safety and health deficiencies or unregulated hazards where no legislation exists to ensure organizational compliance for worker safety. The General Duty Clause places the onus on employers to keep the work environment free of known workplace hazards in the absence of an OSHA regulation. Understanding the reciprocal relationship between employer identification of workplace hazards and employee compliance with employer safety measures, OSHA crafted the *5(b)* legislation under the OSHA Act. OSHA *5(b)* was designed for employee compliance with documented employer workplace standards and countermeasures to ensure the worker's safety and health in the workplace. The Act authorized OSHA to promulgate and enforce safety and health standards through the OSHA Division of Compliance offices throughout the USA. The Act also authorized OSHA to provide free voluntary compliance through education and training measures by the OSHA Division of Education and Training Division. Since 1971, the first enactment of the OSHA Act, safety, and health laws have been passed and regulations issued dedicated to industrial hygiene health hazards and workplace safety (Plog and Quinlan 2012).

What OSHA Does

Workplace injuries and illnesses are expensive to organizations. OSHA plays a vital role in protecting interstate commerce by ensuring the workplace safety and health of employees by holding employers responsible and accountable. Primarily, OSHA accomplishes these objectives by identifying known hazards and encouraging employers to recognize likely safety and health dangers in the workplace, quantifying associated risks, and ensuring that employees are given appropriate equipment and training to combat hazards, whether chemical, physical, ergonomic, or biological. OSHA's organizational efforts are two-fold. OSHA Division of Compliance and compliance safety and health officers (CSHOs) enforce current safety and health regulations through programmed and planned inspections of organizations that may result in fines and penalties due to violations. OSHA Division of Education and Training safety and health personnel provide *voluntary* compliance opportunities, called *surveys or technical assistance* (TAs) for private and public companies, as well as state and local government entities with no fines or penalties under normal conditions. *Voluntary surveys* or TAs requested by an employer do not typically result in fines or penalties if violations found are abated but does offer the company an opportunity to proactively partner with OSHA to prevent workplace incidents resulting in injuries and illnesses. Inevitably, OSHA's role in protecting workers remains the same. However, with emerging technologies and manufacturing strategies come new workplace safety and health hazards and associated risks. OSHA strives to stay ahead of these advancements by establishing new and updated guidelines so that workers in these industries are safe in the workplace (Plog and Quinlan 2012).

OSHA regulations are concentrated in four areas: general industry, construction, maritime, and agriculture. Regulations and guidelines differ among the industries due to the variety of workplace hazards (OSHA n.d.).

General Industry

Codified under US law, 29 CFR 1910 general industry standards set forth governmental regulations designed for those industries not included in agriculture, construction, or maritime. OSHA's general industry standards, directives, and standard interpretations are used to regulate general industry companies, such as hospitals, fire departments, mortician offices and funeral parlors, and foundries.

Construction

Codified under US law, 29 CFR 1926 construction regulations set forth regulations designed for industries involved in construction or construction activities. OSHA's construction standards, directives, and standard interpretations regulate construction industries and general industry activities which fall under construction, such as general and subcontractors.

Maritime

Codified under US law, 29 CFR 1915, 1917, 1918, and 1919, maritime regulations set forth regulations for industries involved in maritime or longshore activities. OSHA maritime standards, directives, and interpretations regulate maritime industries, such as long shoring.

Agriculture

Codified under US law, 29 CFR 1928, agriculture regulations set forth regulations for industries involved in agriculture activities. OSHA agriculture standards, directives, and interpretations regulate agriculture industries.

How OSHA Has Helped

Before the OSHA Act, there were no consensus governmental regulations designed for the protection of workers from occupational safety and health hazards. A direct result of the lack of consensus governmental safety and health regulations, the number of workplace fatalities, injuries, and illnesses numbered in the thousands annually, with many workers suffering fatal injuries daily and acquiring long-lasting chronic illnesses. For nearly 50 years, OSHA has worked tirelessly to improve the working conditions for workers in many industries by making them safer and holding both employers and employees accountable. According to the National Safety Council (NSC), for example, since OSHA has become law, the death rate from work-related injuries has been reduced to four per 100,000, or less than one-third the rate of the previous 50 years. In addition, due to OSHA efforts, US companies have become more competitive in a global economy due to a greater awareness of the cost-effectiveness gained from the prevention of work-related injuries and illnesses.

How OSHA Is Going to Help

Due to its mission statement and 13 core targeted objectives determined by the US Congress, OSHA will play an important role in shaping the future of workplace safety and interstate commerce. As advancements in technology in production, service, and quality move forward, new hazards undoubtedly are going to be introduced into the modern workplace that will place workers at risk. OSHA, industries, and companies will have to work together, forging a partnership in continuing to provide safe workplaces, free from recognized hazards. Industries, with the completion of injuries and illness records (OSHA recordkeeping logs), will assist in identifying emerging injury and illness trends, and will also influence OSHA Compliance targeting.

OSHA Jurisdictions

OSHA, a federal program administered through the Department of Labor (DOL), has jurisdiction throughout the USA and its territories. OSHA standards and regulations cover the most private sector, state, and local governmental employers. For example, all USA island territories, including Puerto Rico, Guam, and the Virgin Islands, are covered under OSHA standards and regulations. Although OSHA is a federal program, the US Congress recognized the need for some states to administer their own OSHA program. These *state-plan states* are federally approved OSHA workplace safety programs that are managed by the individual state or territory. A state-plan OSHA program is monitored by federal OSHA and must be as effective in protecting worker's safety and health in the prevention of workplace fatalities, injuries, and illnesses. The number of federal and state-plan OSHA programs are nearly evenly split among the states and US territories.

Federal Level

There are currently 28 federal operated OSHA programs in the USA and its territories. These programs are located in the following states and territories: MT, ID, ND, SD, NE, CO, KS, OK, MO, AR, TX, LA, MS, AL, GA, FL, WV, OH, PA, WI, DE, DC, RI, MA, NH, and the AS MP and GU territories.

State Level

Currently, there are 22 states with their own OSHA programs plus six states that cover only state and local government workers. These 28 states and territories include WA, OR, NV, CA, UT, AZ, NM, WY, MN, IA, MI, IN, KY, TN, SC, VA, MD, IL, NJ, CN, HI, NC, NY, VT, MN, and the US VI and PR territories.

How the General Duty Clause Is Used

As mentioned in the introduction, the *General Duty Clause* of the OSHA Act imposes on employers a "general duty" to provide a workplace free of "recognized hazards" (Morey 1973). OSHA Division of Compliance can cite a company under the General Duty Clause if an existing deadly or dangerous hazard is not mitigated in the workplace. The General Duty Clause is only used in instances where there is not an OSHA regulation to address a specific hazard. The OSHA Compliance officer, when determining if the General Duty clause applies to an organization, is able to prove the violation when the following four conditions exist:

- Workplace has not been free of hazards that endangered workers.
- Workers and others in the company understood that the hazard existed.
- Hazard danger was or is liable to be deadly or produce severe physical harm.
- A reasonable strategy was available to amend the hazard.

All four of these conditions must be answered in the affirmative in order for a violation of the General Duty Clause to be present.

Conclusion

Signed into law by President Richard Nixon, the passage of the OSH Act by the US Congress promulgated the establishment of OSHA. The mission and task of OSHA is to assure that workplace conditions for both men and women are safe and reliable and that workplace safety regulations are enforced. This is accomplished through training, support, and informational assistance. The OSHA Act was deemed necessary because workplace injuries and illnesses were costly to employers, interfered with interstate commerce, and due to public outcry. The OSHA Act specifically gave OSHA 13 objectives to complete, which include the collection of injury and illness data, providing education and training activities to the general public, developing legislation to provide workers with protection from workplace hazards, and others. OSHA has been very successful in reducing the frequency and severity of workplace injuries, illnesses, and fatalities over its 40 plus years in existence. OSHA adopted many safety and health regulations for the protection of workers. However, the US Congress understood due to emerging technologies in production and manufacturing development knew they could not keep pace with promulgating legislation for the safety and health protection of workers. The General Duty Clause, 5(a)(1), was developed as one of the provisions designed for companies and top leadership to be responsible for the protection of their workers despite the presence or absence of regulatory legislation by OSHA. The General Duty Clause is, therefore, a "catch all" legislative device used by OSHA Compliance to cite companies that expose workers to workplace hazards where no legislation exists.

References

Morey, R. S. (1973). The general duty clause of the Occupational Safety and Health Act of 1970. *Harvard Law Review, 86*(6), 988–1005. The Harvard Law Review Association. Retrieved from https://www.jstor.org/stable/1340085.

OSHA. (n.d.) *Introduction to OSHA*. Occupational Safety and Health Administration. Retrieved from

https://www.osha.gov/dte/outreach/intro_osha/intro_to_osha_english/slide1.html
OSHA-3125. (2000) *Ergonomics: The study of work*. US Department of Labor, Occupational Safety and Health Administration. Retrieved from https://www.osha.gov/Publications/osha3125.pdf
OSHA-About. (n.d.) *About OSHA*. US Department of Labor, Occupational Safety and Health Administration. Retrieved from https://www.osha.gov/aboutosha
Plog, B. A., & Quinlan, P. J. (2012). Respirable crystalline silica. In *Fundamentals of industrial hygiene* (6th ed.). Itasca: National Safety Council. Retrieved from https://www.osha.gov/silica/Table1sect1926.1153.pdf.

Further Reading

Clemco. (2016). *Respirable crystalline silica: Its history, associated disease, and the new OSHA standard – Understanding the new regulations*. Clemcoindustries.com. Retrieved from http://www.clemcoindustries.com/images/pdfs/Respirable_Crystalline_Silica.pdf
Finkel, A. M., & Sullivan, J. W. (2011). A cost-benefit interpretation of the "substantially similar" hurdle in the congressional review act: Can OSHA ever utter the e-word (ergonomics) again? *Administrative Law Review, 63*(4), 707–784. American Bar Association. Retrieved from https://www.jstor.org/stable/23065488.
Fuge, C. (2002). The ergonomics regulation roller coaster. *IRMI*. Retrieved from https://www.irmi.com/articles/expert-commentary/the-ergonomics-regulation-roller-coaster
Goetsch, D. (2019, updated). *Occupational safety and health for technologists, engineers, and managers* (9th ed.). New York: Pearson.
Middlesworth, M. (2012). How to recognize ergonomic risk factors in the workplace. *ErgoPlus*. Retrieved from https://ergo-plus.com/ergonomic-risk-factors/

Investigations: Polygraph Use

Frank Chen
John Jay College of Criminal Justice,
New York, NY, USA

Keywords
Deception · Lie detection · Polygraph

Definition

The polygraph measures blood volume, breathing, pulse, and sweat rate of examinees to guide the polygraphist in determining truth and deception.

Introduction

Since the inception of deception detection, physiological stress was always a problematic measurement. Heightened stress responses are often misinterpreted as deception because there is not a single distinctive stress response for deception. Unless this distinctive stress response exists or is identified, no machine would be able to detect lies, specifically the polygraph. When guided by the polygraph, the only capable lie detectors are the prepared polygraphists who carefully study their examinee's physiological responses to control and relevant questions and attempts to beat the machine.

A Brief History on Truth and Deception

Deception started before our first language as humans and played a critical role in the personal gain and survival of many species. For example, anglerfishes use a shiny lure in the shape of a tasty juicy worm above their heads to attract other fish while hunting in the dark sea. Hognose snakes feign death and secrete a foul odor to warn predators that consumption of itself may lead to dangerous diseases, illnesses, or death (Owen 2015). Each example illustrates a different purpose of deception, with the anglerfish's. method attracting others while the hognose snake's method deterring others. We also use deception to attract or deter others, as we can also hang shiny tasty lures above our heads to attract others or secrete foul odors when threatened but that would probably produce mixed results. Regardless of our deception methods, we lie, trick, and deceive others out of fear, personal gain, or habit. "The ability to mislead or deceive probably carried an evolutionary advantage just as did fleetness of foot or the possession of an opposable thumb" (Lykken 1998). Since the birth of this evolutionary advantage, it is very likely that deception detection followed shortly afterward.

Before the recognized importance of deception detection, there was a magical and, at times, a religious belief that the honest would always emerge victorious and the deceptive would

always be defeated. This belief existed in trails by combat, where the honest fighter was blessed based on their truthful character by a higher power and the deceptive fighter would be cursed, weakening them in combat and setting them up for defeat. The honest would also survive in trials by ordeal, such as walking on fire or dipping their arms in boiling water. The assumption was that under these trials, only the deceptive are punished and the truthful are protected (NTLS 2015).

The search for truth started as early as 300 B.C., where Bedouins of Arabia developed a hot metal spoon method where suspects of a crime were required to lick a hot metal spoon three times to determine if they were truthful or deceptive. This ritual was known as the "Bisha," and the assumption behind this truth test was for persons who were deceptive would have a dry tongue and after licking the hot metal spoon would then have a burnt tongue. If the person was honest, their tongue would be moist and not dry, which would protect them from the hot spoon. Accused persons with a burnt tongue after this ritual would be found deceptive and guilty for the crime accused (NTLS 2015).

This salivary physiological response was common in other cultures as well and was also used in China, except the accused were required to chew rice instead of licking hot metal spoons. When the accused chewed and spat out the rice, rice that stayed on the accused's tongue indicated deception. The assumption was that if the accused was innocent, their tongue would be wet and not dry because there was no reason to stress over the test if they were truthful (Leafloor 2014). Similarly, when we are under situations of high stress or deception today, one of our immediate physiological reactions is the dryness of throat, causing us to swallow as a response. Other physiological responses include increased breathing, pulse rate, and sweat, which of course led to other deception detection techniques.

African tribes used a smelling technique, where the accused stand around an African medicine man in a circle. The medicine man continuously smells the necks of the accused while delivering "blood-curdling" shouts along with another feverish smell of the accused (Trovillo 1939). These shouts heighten the stress levels of the accused, making them sweat uncontrollably and excessively. In this deception detection technique, it uses perspiration as the deception physiological response, and thus the person who sweats the most must be deceptive.

As you probably guessed, the aforementioned methods were not very reliable and often led to innocents punished for crimes they did not commit. Thankfully, modern-day deception detection techniques advanced beyond the use of hot spoons, rice, or a strong sense of smell. They start with nonverbal indicators, unique to each individual's character and can range from rubbing or scratching the nose, eyes, ears, or the back of the head. Other indicators include grooming, heavy breathing, or cracking fingers. These nonverbal gestures are unique because they are learned through associations with others and start as early as childhood. However, these nonverbal indicators are not signs of deception; they are only signs of stress and are often misinterpreted as deception, similar to the techniques identified earlier. The distinction between stress and deception is assumed through our human behavior analysis skill, which is challenging to measure and accurately document. For starters, determining truth and deception depends on your own truthful or deceptive personal character and requires you to be well aware of your physiological stress responses. If you are truthful most of the time, you should search for truthful cues and if you are deceptive most of the time, you should search for deceptive cues. You can also be a truthful person and search for deception cues and vice versa but that might require extra practice. It might be easier for some of us to interpret verbal, nonverbal, and written forms of communication with the truthful or deceptive character and cues they are most familiar with – themselves or an intimate other. The act of measuring stress to assume deception is the function of the Lie Detector machine, also known as the polygraph.

The Genesis of Lie Detection Machines

The first prototype of the modern-day polygraph started with the analysis of blood flow within

a deceptive person. In 1730, Daniel Defoe's essay on prevention of street crime wrote how "Guilt carries fear always about with it; there is tremor in the blood of the thief" (Grubin and Madsen 2005). Defoe determined how unequal pulse changes and heart palpitations are strong indicators for deception during questioning which started in the early twentieth century with Austrian Benussi. Benussi's research identified the relationship between blood pressure, pulse, and breathing rate now known as the Benussi ratio. Using the Benussi ratio, William Marston's systolic blood pressure deception test became the prototype for the modern-day polygraph. Marston's polygraph prototype used a standard blood pressure cuff and stethoscope while assuming the relationship between specific lie responses and changes in systolic blood pressure.

Marston's prototype polygraph was submitted as evidence in the Supreme Court case Frye v. United States, 1923. Accused of robbery and murder, James Frye took Marston's lie detector test and passed, which assumed Frye to be innocent. The trial judge refused to allow the admissibility of Marston's apparatus as scientific evidence based on questionable validity from the scientific community and is now known as the Frye standard test. Since the use of Marston's lie detection device in Frye v. United States, it attracted the attention of other professionals and eventually became the modern-day polygraph.

Larson created the first modern polygraph apparatus in 1921 that transcribed the physiological responses of blood pressure, pulse rate, and respiration (hence the name polygraph which means many writings). This first model of the polygraph proved successful and was later advanced to be portable by Leonarde Keeler, Larson's disciple. Keeler furthered the portable polygraph and improved it to measure pulse rate, blood volume change, breathing, and sweat in 1939. Keeler's model of the polygraph was the first lie detection instrument purchased by the Federal Bureau of Investigation and became the first prototype for the modern-day polygraph. Since the creation of the polygraph, professionals who were heavily involved in determining truth and deception merited its utility.

Polygraph Function

The polygraph records physiological responses of an examinee under stress. Under high levels of stress, which causes physiological responses to become more apparent, the sympathetic nervous system kicks in. The sympathetic nervous system is one of the two parts of our central nervous system and activates when we sense danger (also known as Walter Cannon's fight/flight response) (Brown and Fee 2002). Over the years, Bradford's fight/flight response was widely referenced and is now sometimes referred as "the four Fs" (fight, flight, freeze, and our popular and offensive four-letter word starting with an F and ending with a K). While experiencing one of the four Fs, the polygraphist determines truth and deception through interpreting polygraph charts and nonverbal behaviors during sympathetic stress. Some example of nonverbal behaviors include and are not limited to (a) pupil dilatation; (b) inhibition of salivary glands, waste elimination, and gastrointestinal tract; and (c) increased activity in breathing, sweat glands, and heart rates. These nonverbal behaviors could be deception indicators – some of which include "gaze aversion, increased or decreased movement, longer and more frequent pauses, a slower speech rate, hesitations, and speech errors" (Grubin and Madsen 2005). These categories of nonverbal behaviors are indicators of deception unique to each individual, thus requiring the polygraphist to study and determine baseline behaviors prior to assuming stress responses as deception.

So how does the polygraph measure physiological stress to assume deception? The modern-day polygraph measures breathing, heart rate, blood volume, and sweat with "(1) two expendable bands positioned around the thorax and the abdomen, measuring respiration, (2) two electrodes attached to the inside of the hand, measuring electrodermal activity, and (3) an inflatable cuff positioned around the upper arm registering blood pressure" (Meijer and Verschuere 2010). According to Bruno Verschuere, "skin conductance response is the most frequently applied and best validated measure for the detection of concealed information" (2010). Other scholars

argue that breathing, heart rate, or blood volume to be stronger indicators of deception. Since there is no unique pattern or physiological response that would determine truth and deception, the polygraph is simply an instrument that records the physiological responses to guide a polygraphist in determining truth and deception.

Physiological readings are always accurate, but the challenge is proper interpretation of the readings (Aftergood 2000). The Supreme Court Case United States v. Scheffer in 1998 stated that "there is simply no way to know in a particular case whether a polygraph examiner's conclusion is accurate, because certain doubts and uncertainties plague even the best polygraph exams." According to Lykken, "We have already noted that for there to be an instrument that literally detects lying, there must be a specific lie response, a distinctive involuntary, bodily reaction that everyone produces when lying but never when telling the truth. There will never be a Truth Verifier (lie detector) until a specific lie response can be identified" (Lykken 1998). In short, since there is no specific lie response, no instrument will be able to detect lies.

Therefore, since the creation of the polygraph, there was an acknowledgment on how the polygraph is not a lie detector machine. There was also the growing concern that the polygraphist will be subject to bias and is not immune to uncontrollable factors that may alter their discretion in determining truth and deception. Nevertheless, the polygraph is still termed as the "lie detector test" with many researchers challenging the validity of its capabilities in determining truth and deception. The truth is that the polygraph does not determine truth and deception; it is the polygraphist conducting the exam with the aid of the polygraph and through the proper use and delivery of interview questions.

Phases of the Polygraph Exam

The polygraph exam is only successful if the polygraphist properly delivers each phase. Prior to the first phase (pretest), the examinee must be formally scheduled and given ample time in advance. This will allow truthful examinees to relax and calm down before the exam while heighten the stress of deceptive examinees. The first phase is the pretest interview and cannot be skipped or ignored at all costs. During the pretest interview, the polygraphist will introduce the examinee to the examination room and equipment, obtain informed consent for testing, and familiarize the examinee about the exam process, so there are no surprises throughout the exam. The polygraphist must be transparent and be very clear to the examinee about the process, the machine attachments, and recordings to ensure exam confidence. Lastly, the examinee must feel comfortable in the room, such as not feeling too hot or cold or have a need to use the restroom as any discomfort may distort polygraph chart results. This phase normally should take up to 20–30 min (Reid and Inbau 1977).

The polygraphist will demonstrate how the polygraph works through a mock test, where the examinee is instructed to tell a lie and the examiner will show that the polygraph has caught the lie and provide evidence of its accuracy. The polygraphist in this phase can also determine the examinee's behavior, character, and truthfulness "based on the examinee's demeanor and responses in the pretest interview and during the charting" (National Research Council 2003).

Depending on the type of interview, the polygraphist can also personalize the pretest interview by using psychometric techniques such as graphology, House-Tree-Person test, psychogeometry, the Thematic Apperception Test, and others to determine baseline behavior and establish rapport and theme. These psychometric techniques are not designed to determine truth or deception or to be a substitute to the polygraph. Psychometrics are used at the discretion of the polygraphist, which, if used incorrectly, may negatively affect the outcomes of the polygraph readings and interpretation. The purpose of the pretest interview is also to relieve an innocent examinee's stress while heightening the sympathetic arousal of a guilty person. Therefore, the polygraph not only allows a polygraphist to determine an examinees physiological response and establish rapport but

also indoctrinate the mind-set of the examinee that if they are innocent, they will be deemed innocent and if deceptive, they would be found guilty (Lewis and Cuppari 2009).

The pretest interview can also be an opportunity for the polygraphist to use other rapport-establishing techniques, such as Richard Bandler's Neuro-Linguistic Programming (NLP). NLP has evolved over the years since its inception in the 1970s. The original purpose of NLP was to understand others better through studying eye movement gestures. Bandler categorized our five senses (sight, hear, smell, taste, and touch) into visual, auditory, and kinesthetic (smell, taste, and touch). Based on your eye direction when answering questions (top, middle, or bottom), you were a visual, auditory, or kinesthetic learner. Additionally, looking left or right while looking top, middle, or bottom would indicate truth or deception (Bandler et al. 1979). Regardless of the original intention of NLP, it is now employed as a method to establish theme in communication and in the pretest of the polygraph exam. There are many methods to establish theme, but one of the easiest methods is to determine what type of learner an examinee is and to use the words associated with the learning method. For example, if the polygraphist finds their examinee to be a visual learner, they would use visual-oriented words such as "I see what you mean." If the examinee is an auditory learner, the polygraphist would use auditory-oriented words such as "sounds good." Lastly, if the examinee is a kinesthetic learner, the polygraphist would use kinesthetic words such as "smells fishy" or "feeling salty." This technique as with many other psychoanalysis techniques is a pseudoscience and is not always scientifically proven to work. Regardless, if it actually works or not, these techniques would boost the polygraphist's confidence in determining truth and deception. It is this immeasurable confidence that drives the polygraphist to hold their breath longer than the examinee, to separate and exhaust deceptive examinees from the truthful. In short, this NLP rapport technique is one of the many theme techniques professionals can use to establish rapport and can be used in the pretest phase of the polygraph exam.

In the in-test phase, the polygraphist must communicate every question clearly and carefully as shared in the pretest phase. Polygraph exam questions cannot be ambiguous or use sensitive words related to the crime. For example, in a child molestation case, the polygraphist should not use the word "rape" or "pedophile" but instead use terms such as "inappropriately touch" or "sexual intercourse." The polygraphist should also not use technical jargon that the examinee would not understand such as fellatio, as it would lead to confusion and inaccurate polygraph writings. Questions should also not be lengthy as it would dampen the stress levels of deceptive examinees and stress out honest examinees.

Three important types of questions asked during the in-test phase are control, relevant, and irrelevant. Before the test begins, the polygraphist will read their list of questions to the examinee in any order to ensure they understand each question. This list of questions will have a mix of control, relevant, and irrelevant questions. The sequential order of control, relevant, and irrelevant questions is extremely important and changes based on the type of interview. There are many standardized test orders, some of which also have additional instructions. For example, by assigning two relevant questions one after another and asking the examinee to answer truthfully to one and deceptively to another is known as the positive control test. By asking examinees to deceptively answer every control question is known as the directed lie test. Regardless of the question set, the polygraphist will inform the examinee that only the questions read to them will be asked and that there are no surprise questions. The most well-known polygraph question set is the control question test, which focuses on physiological responses to control and relevant questions.

Control questions are vague questions that cover events from previous life experiences and are recommended to be related to the crime accused. Control questions are meant to make the subject uncomfortable because the questions are designed to make it difficult for the examinee to answer "no." For example, in a crime related to robbery, the examinee would be asked, "in your

entire life, have you ever stole something?" For most of us, we take things from time to time and would not classify the action as stealing. For example "borrowing" scissors or other office supplies from our colleagues and "forgetting" to return it. Although the intention to steal was never there, the action of taking other peoples' possession without permission can be labeled as stealing for some and not for others. For individuals who would label this action as stealing, they would experience physiological stress when confronted with this control question. "Control questions are designed to provide the innocent suspect the opportunity to become more concerned about questions other than the relevant questions and to produce stronger physiological reactions to control questions. If the subject shows stronger physiological reactions to the control as compared to the relevant question, the test outcome is interpreted as truthful. Stronger reactions to the relevant questions indicate deception" (Lykken 1998).

Relevant questions are questions that are directly related to the crime at hand. If the suspect has committed more than one crime, the crime that is the most serious will stress them out the most, providing the strongest physiological response. For example, if the suspect was involved in three different drug-related crimes and one out of the three involved murder, the murder case is most likely going to occupy the suspect's concentration, focus, and effort in concealing deception. The other two drug-related crimes would be the least concern to the suspect and produce lower stress responses. This is known as the anti-dampening concept and is defined by Lykken as "a person's fear, anxieties and apprehensions are channeled toward the situation which holds greatest immediate threat to his self-preservation or general well-being, (and that there is) an ability within us to tune in that which way indicate trouble or danger by having our sense organs and attention set for a particular stimulus and oriented in a manner that will dampen any stimulus of lesser importance" (1998). For example, if a respectful law-abiding student is taking a polygraph exam for a job opportunity in the federal government and were previously engaged in "agriculture," questions related to experimenting with cannabis would heighten the student's responses knowing that it would disqualify them from job employment. Questions related to murder or stealing would not generate strong physiological responses because the student's entire focus is on their past cannabis experiences. In sum, the anti-dampening concept will affect responses to relevant questions depending on the situation, examinee's concentration, and focus.

Irrelevant questions are questions that are completely irrelevant to the crime under investigation. Sample irrelevant questions are "Is your name Phil?", "Did you ever ride a bike?", and "Are you in New York right now?" "The primary purpose of the irrelevant questions is to ascertain the subject's normal reactions – his 'norm' – under test conditions" (Reid and Inbau 1977). The normal reactions are important because it is also the examinee's baseline behavior. Although irrelevant questions help the polygraphist establish the norm behavior of their examinee, the problem is that if the examinee lies on the irrelevant questions and they are not confronted on the lie, the examinee will believe they can evade detection when confronted with relevant questions. As stated earlier, depending on which set of questions produces higher levels of physiological response, the subject will be deemed truthful or deceptive. If the subject shows higher physiological responses to the control questions, they are deemed truthful. If the subject shows higher physiological responses to the relevant questions, they are deemed deceptive. The actions taken by the examinee to alter their physiological responses to control and relevant questions to misguide the polygraphist is known as "beat the machine."

Beat the Machine

"Beat the machine" is defined as the examinee's attempt to manipulate the results of polygraph readings through hidden methods undisclosed to the polygraphist. An estimate of 20% of examinees often try to "beat the machine" through

various methods such as voluntary muscular movements to mislead the polygraphist during questioning (Reid 1945). These muscle contractions are also known as peripheral resistance, where based on muscular activity, the resistance of blood flow increases or decreases. Reid's research shows that these voluntary unobserved muscular movements have the following properties: (a) all typical blood pressure responses can be produced voluntarily and at will, (b) voluntary and at-will blood pressure responses can be differentiated from true indications of guilt, and (c) recorded evidence of muscular evidence is an indicator of deception (1945). In short, unobserved muscular movements during polygraph tests are methods to beat the machine, specifically when asked control questions.

The best advice to beat the machine is to identify the control questions and to alter your physiological reaction to the control questions. This action will make it difficult for the polygraphist to differentiate between control and relevant question physiological responses. A method to alter your physiological reaction is through self-inflicted pain or tightening your muscles to control physiological responses. If you are unsure of how to identify the control questions to beat the machine, you can also relax, hold your breath, or do anything to calm yourself when you are asked the relevant questions. Any method that would cause the polygraph charts to show similar physiological responses to control and relevant questions will allow you to beat the machine successfully. Being mindful of methods to beat the machine will help subjects pass the polygraph test, as "a high proportion of honest people will fail lie detector or honesty tests when they rely on their truthful answers to demonstrate their innocence or good character. Meanwhile, the more clever of the villains will employ countermeasures to ensure that they manage to pass" (Lykken 1998).

After the in-test phase is the posttest phase, where the polygraphist will have the results of the exam immediately after the in-test phase. The polygraphist will determine the examinee as deceptive, honest, or inconclusive. Deceptive is determined by the examinee showing consistent and stronger physiological responses to relevant questions. Honest is determined by the examinee showing consistent and stronger responses to control questions. Inconclusive is when the polygraphist is unable to determine if the examinee is deceptive or honest. Deceptive and honest exam results are determined by a numerical scoring system, traditionally scoring deceptive responses as negative points and honest responses as positive points (Synnott et al. 2015).

Measuring Polygraph Validity

Measuring polygraph validity is extremely challenging and if not, more confusing and complicated given the required learning curve of accurately interpreting and transcribing polygraph charts during testing. Although assumingly used for determining truth and deception, the polygraph is only an instrument that would guide the polygraphist in reassuring their discretion. Empirical studies show that "in experimental settings, the ability of the average person to catch a liar is rarely above 60%" (Grubin and Madsen 2005). Additionally, the United States Justice Paul Stevens determined the polygraph only having an 85% to 90% accuracy reliability rate with critics estimating a 70% accuracy rate (Gershman 1998). Given the percentages here, it appears that the lie detection rate between an average person and the use of a polygraph can be up to 25% when using the polygraph. Do not let these percentages fool you, as "the clinical judgment of a polygraph examiner is no more valid than that of any other observer, just as subject to bias and prejudice, and probably wrong nearly 50% of the time" (Lykken 1998). Empirical research on lie detector accuracy rates and its percentages are best explained by Benjamin Disraeli's quote "There are three kinds of lies; lies, damn lies, and statistics."

Testing Polygraph in Laboratories

Critics who attempt to debunk the validity of the polygraph often test its legitimacy through controlled laboratory settings. Laboratory experiments on measuring polygraph validity often

produce misleading results given the nature of the experiment. Laboratory settings offer a completely different environment and experience to examinees compared to real-life polygraph exams. "Laboratory studies that are based on non-emotional orienting responses absolutely fail to replicate the field conditions that elicit emotional defensive responses wherein both the guilty and innocent examinee's primary emotion is 'fear' of the consequences if found deceptive which in criminal cases could result in imprisonment" (Matte 2011).

Other polygraphists drew the same conclusions regarding polygraph laboratory studies. Lykken believed that laboratory studies "have serious disadvantages for predicting lie detector accuracy in real-life criminal investigations" (Lykken 1998). The first disadvantage is that volunteers do not accurately represent criminals in real life and, thus, will not express or experience real concerns to the lies they are instructed to tell. The second disadvantage is that there are no perceivable consequences for volunteers if they fail the polygraph exam. The third disadvantage is that laboratory polygraph mock studies occur shortly after a mock crime occurs. This does not happen in the real world, where polygraph testing may occur days or even weeks after a crime occurs. Therefore, we can conclude that laboratory tests cannot determine polygraph validity.

Employee Polygraph Protection Act of 1988

According to The Employee Polygraph Protection Act of 1988, all private employees are protected from an employee requirement to take the polygraph exam. Employers cannot request or even suggest employee candidates to take the polygraph exam, nor are they allowed to terminate an existing employee because of a refusal to take a polygraph exam. The Employee Polygraph Protection Act of 1988 does not apply to federal, state, or local government agencies, nor does it apply to professions regarding national defense.

Currently, the polygraph is used to screen applicants for government positions and is known as the applicant screening test. The polygraphist follows the same process as they would normally and work off multiple question lists. The examinee is tested to see if their physiological responses remain constant across all content areas, from drugs to violence to stealing and other acts that would disqualify them for employment. Any content area that draws stronger physiological responses will be asked repeatedly with longer pauses to determine deception. If the polygraphist is convinced the examinee is deceptive, they can stop the polygraph and directly confront them about their deception. If the examinee continues to deny deception, the polygraphist will continue with the test and return to the sensitive content area later. As you probably guessed, many examinees also try to beat the machine. The most important fact to remember in preparation for the polygraph exam is your belief in the machine. "Once you believe in the machine, it works. Once you believe in the charts, it works. The polygraph does not believe in you, but you will believe the polygraph" (Lykken 1998).

Conclusion

Although known as the lie detector machine, the polygraph would only serve as a guide for the polygraphist to determine truth and deception as a Microsoft PowerPoint presentation would serve as a guide for a presenter. It is not the flashy graphics or song cues in a PowerPoint presentation file that makes the presentation or lecture a living masterpiece – it is the presenter himself or herself. As for the polygraph, it is not its physiology measurement capabilities, it is the polygraphist himself or herself. The polygraph only appears to be the better lie detector because of its scientific presence and physiology recording function. When we combine the polygraph presence with our naïve dependency on technology, we believe in the machine. It is true about the polygraph that it is close to perfect in measuring physiological response, but it still requires a person to use their discretion to determine truth and deception given the unique character and nature of each individual person.

Cross-References

- ▶ Personnel Security: Hiring
- ▶ Personnel Security: Selection
- ▶ Physical Security: Best Practices

References

Aftergood, S. (2000). Essays on science and society: Polygraph testing and the DOE National Laboratories. *Science, 290*, 939–940.

Bandler, R., Grinder, J., & Andreas, S. (1979). *Frogs into princes: Neuro linguistic programming*. Moab: Real People Press.

Brown, T., & Fee, E. (2002). Walter Bradford Cannon: Pioneer physiologist of human emotions. Retrieved 16 May 2015, from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1447286/

Gershman, B. (1998). Lie detection: The Supreme Court's polygraph decision. *New York State Bar Journal*. Retrieved 5 May 2015, from http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1613&context=lawfaculty

Grubin, D., & Madsen, L. (2005). Lie detection and the polygraph: A historical review. *The Journal of Forensic Psychiatry & Psychology, 16*, 357–369.

Leafloor. (2014). http://www.ancient-origins.net/myths-legends/truth-about-lie-detection-ancient-and-modern-times-002125

Lewis, J., & Cuppari, M. (2009). The polygraph: The truth lies within. *The Journal of Psychiatry & Law, 37*, 85–92.

Lykken, D. (1998). *A tremor in the blood: Uses and abuses of the lie detector*. New York: Plenum Trade.

Matte, J. (2011). Commentary on: Horvath F, Palmatier JJ. Critique of Horvath-Palmatier laboratory study on effectiveness of exclusive v. non-exclusive control questions in polygraph examination. J Forensic Sci 2008; 53(4):889–99. *Journal of Forensic Sciences, 56*(6), 1664–1667.

Meijer, E., & Verschuere, B. (2010). The polygraph and the detection of deception. *Journal of Forensic Psychology Practice, 10*(4), 325–338. https://doi.org/10.1080/15228932.2010.481237.

National Research Council. (2003). *The polygraph and lie detection*. Washington, DC: The National Academies Press. https://doi.org/10.17226/10420.

NTLS. (2015). http://discoversinai.net/english/bisha-the-ordeal-by-fire-of-the-bedouin/8734

Owen, J. (2015). https://news.nationalgeographic.com/2015/10/151019-playing-dead-frog-possum-toad-animals-behavior-science/

Reid, J. (1945). Simulated blood pressure responses in lie-detector tests and a method for their detection. *Journal of Criminal Law and Criminology (1931–1951), 36*(3), 201–201.

Reid, J. E., & Inbau, F. E. (1977). *Truth and deception: The polygraph ("lie-detector") technique*. Baltimore: Williams & Wilkins.

Synnott, J., Dietzel, D., & Ioannou, M. (2015). A review of the polygraph: History, methodology and current status. *Crime Psychology Review, 1*(1), 59–83.

Trovillo, P. (1939). History of lie detection. *The Journal of Criminal Law and Criminology, 29*(6), 848–881.

Further Reading

Gordon, N. J., & Fleisher, W. L. (2017). *Effective interviewing and interrogation techniques*. Amsterdam: Elsevier Academic Press.

Lykken, D. (1998). *A tremor in the blood: Uses and abuses of the lie detector*. New York: Plenum Trade.

Reid, J. E., & Inbau, F. E. (1977). *Truth and deception: The polygraph ("lie-detector") technique*. Baltimore: Williams & Wilkins.

I

Investigations: Sexual Assault

Rifath Ali[1] and Sidra Perveen[2]

[1]Department of Safety, Security, and Emergency Management, College of Safety and Justice, Eastern Kentucky University, Richmond, KY, USA

[2]King Edward Medical University, Lahore, Punjab, Pakistan

Keywords

Crime · Crime reconstruction · DNA evidence · Forensic medicine · Rape · Sexual abuse · Sexual assault · Sexual violence · Violence against women

Definition

Legal, sociopolitical, clinical, and moral definitions differ significantly, but generally in most jurisdictions, any unwanted sexual attack or attempt which may or may not involve force – such as fondling, grabbing, or verbal threats – is considered a sexual assault, while rape is an aggravated form of sexual assault in which penetration is involved.

Introduction

The investigation of sexual assault differs significantly from other criminal investigations in many ways. Nonreporting and delayed reporting are very common in sexual assault cases. Even the victims who choose to report the crime may not be in a physically and mentally stable condition. False allegations are also a common phenomenon.

On the other hand, physical and forensic evidence needed to prove assault deteriorates quickly with time. Following standard protocols used for investigating other crimes can be a dangerous pitfall in sexual assault cases. This necessitates a great deal of care on the part of the investigator, without compromising time efficiency, to collect evidence, and deal with the victim and alleged perpetrator with utmost care. For investigators who are new to sexual assault investigations, the preconceived notions derived from films, fictions, or hearsay can cloud their judgment and imperil investigations that are often very different in reality.

Investigation of sexual assault is a process by which the investigator determines what happened and can reconstruct the crime scene with suitable explanations derived from the victim, eyewitness, and offender statements and corroborated by physical and forensic evidence. For investigating sexual assault, only criminal violations of a penal code enforceable by the courts are relevant.

The criminal law definitions of sexual assault differ across different jurisdictions. Therefore, investigators should adhere to legal interpretations of the statute in consideration when investigating a sex-related crime (Morgan and Kena 2018; Kruttschnitt et al. 2014).

The elements of sexual assault investigations can be classified into four broad categories: (1) investigative response, (2) victim management, (3) reconstruction and physical evidence, and (4) analyzing offender. These broad categories need to be examined in detail to enable an investigator to probe and prosecute sexual assault cases in an effective manner (Savino and Turvey 2011).

Investigative Response

Sexual assault investigations start with first responders when a crime is reported. The next phase is the preservation of the evidence at the crime scene and its management in a manner that vital elements that can impact investigation and trial are carefully handled. The investigators then begin their investigation by examining the crime scene thoroughly and recording statements of victims and perpetrators, if possible. A cohesive and comprehensive response significantly increases the chances of solving the crime, apprehending the offender, and sustaining a trial.

First Response

Savino and Turvey (2011) argue that the first response by its very nature is a rush to the crime scene, which is often disorganized in any crime. In sex-related crimes, three additional factors are in play, and improper handling can lead to inaction. First, any personal issues of the investigator and the intimate nature of the crime can lead to an uncomfortable environment for the investigator. Second, improper training often results in under documentation because the investigators believe that the emotional nature of the victim may result in a contradictory statement, thereby rendering future prosecution difficult. Third, the improperly trained investigator often under collects the physical evidence for the same fear of contradiction noted above. It is practical to know that Andrew Silke (2001) reviewed Brent Turvey's book, *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, contending that Turvey uses inductive reasoning at the crime scene. Working backward from a conclusion is not best practices for most investigators, and this criticism of Turvey is not exclusive to Silke. Turvey's investigative process, however, is widely accepted.

The first responsibility of a sex crime investigator is to determine what happened and whether or not what happened constitutes a crime. If so, the detective should proceed to arrest the persons in violation of the law. The investigator should always assume that the case will go to trial and therefore preserve evidence accordingly. There are three critical aspects for the investigator:

(1) interview the officer who filed an initial report or reached the crime scene first, (2) preserve the crime scene, and (3) proceed to a preliminary interview of the victim with witnesses and officers present. The investigator should make a case book of relevant information, tips, and leads.

The investigator should be well versed in the relevant law to understand what evidence needs to be collected and preserved in order to prove a case in the court. The suspects can only be arrested if there is "probable cause" that a crime has been committed or is being committed by the person arrested. This can only be justified in the court with a detail of the facts and circumstances that require an arrest. A mere suspicion does not constitute probable cause (Savino and Turvey 2011). Chisum and Turvey (2011) describe the actions the first responder should complete before the arrival of the investigator. These include making the crime scene safe by securing the crime scene and restricting access to it, rendering aid to the victim, keeping victims, suspects and witnesses separate from each other, and protecting evidence from deterioration. The attitude of the investigator should be helpful and encouraging. A dismissing attitude can easily put off witnesses and victims from seeking help and cooperating with the investigation. The investigator should be aware of the concerned crime lab and forensic help required for the case. Forensic evidence may often make or break the case. Therefore, a good investigator should know the different types of forensic evidence and sciences. This enables effective and efficient coordination with the forensic team sent to the scene. Some crime labs face serious backlogs, and collected DNA evidence may not turn into objective crime data because of non-pursuance by investigators. Lab personnel may only give importance to the case being pursued, thus leaving many rape kits untested (Savino and Turvey 2011).

Preservation and Management of Crime Scene

Crime scene preservation and management is an essential first response consideration for the investigator. Large metropolitan police departments have special squads and teams to deal with different crimes. Of these, sex crime units provide the expertise needed to investigate sex crimes, but very often, a single crime scene may involve multiple units. In cases involving homicide, burglary, and sex crimes, various units need to coordinate. National Forensic Science Technology Center (NFSTC) details various crime scene procedures and protocols that investigators should follow to preserve and protect the crime scene. The document emphasizes establishing leadership and control on the investigation and its media coverage without compromising the crime scene in any manner (NFSTC 2013).

Following the initial receipt of information and persons involved, according to the NFSTC, the involvement of the safety of law enforcement personnel is determined. A scene assessment is then conducted to ascertain site safety issues and search warrant requirements. The investigator should then conduct a "walk-through" of the crime scene if it does not interfere with the evidence. Some crime scenes require immediate documentation and preservation of evidence before a walk-through is done. Note-taking and logging the entry/exit of persons present at the crime scene is essential and very helpful in subsequent identification and prosecution of the suspects. After this initial assessment of the crime scene, the investigator should proceed to constitute a team of personnel who are well trained in the processing of the crime scene. The investigators and scene-processing team should take measures to avoid hazards and cross-contamination in order to preserve the evidence. The processing of the scene requires extensive documentation. The scene should be photographed, and photography should be supported with video of the scene. Sketches and distances of the evidence and important locations should also be carefully documented to avoid any contradiction in the future. If the circumstances demand following a procedure different from the standard protocols, then such circumstances should also be noted and documented at the scene. Sketches should be drawn to scale, if possible.

Next follows the collection of evidence, methodically, and systematically. Prioritization is important. The most "transient evidence" should

be collected first, followed by the least intrusive, and then the most intrusive evidence should come last. A crime scene search is of four types: (1) lane or strip search, (2) grid search, (3) zone search, and (4) spiral search. In lane or strip search, the investigators walk in parallel along predetermined lines or strips in the same direction. If the searchers go perpendicular after completing the lane search, then this is known as grid search. The time taken is doubled. However, the advantage is a more thorough and accurate search. In zone search, the area is divided into adjacent zones, which are then searched separately. The investigators may choose to move in a spiral inward or outward to search, but the outward spiral method can result in loss of evidence when the searcher is moving towards the center initially to search. In cases involving unique evidence items that need handling by trained professionals, the non-expert handlers should wait and allow the appropriate personnel to collect and preserve evidence. Flammable liquids that can burn and destroy the whole crime scene need special handling to avoid damage to people as well as property.

Similarly, bodily fluids such as blood, saliva, and semen, which are essential for DNA profiling, should only be handled by an expert or trained professionals. Bombs, explosives, firearms, ammunition, and voluminous documentation are other areas where subject matter experts can be significant in a safe but efficient evidence collection. Packaging and marking of these types of evidence should also be done by trained staff. Tool mark evidence, for instance, is collected by using castings. *Trace evidence*, the evidence composed of tiny materials found at the crime scene such as hair, pollen, stains, requires specialized equipment for collection, packaging, and storage. Footwear impressions, motor vehicles, and electronic gadgets need different resources to preserve evidence related to the crime (NFSTC 2013; Chisum and Turvey 2011).

Crime scene investigation is the process of using crime scene evidence to establish facts of the case scientifically. The investigator examines the physical evidence, statements of victims, suspects, and witnesses, and then goes beyond the evidence to connect the dots and establish what happened, based on facts. Savino and Turvey (2011, pp. 139–173) mention that the investigation begins with determining the *point of contact*, which is the point where the suspect initially contacted the victim, and which may not be the actual crime scene. The *primary crime scene* is the location or point where the principal criminal activity took place. This is the scene that gives the most physical evidence and is generally the scene where the suspect probably spent the most time during the crime. In the case of multiple crimes, the primary crime scene for sexual assault may be different from other crimes, such as homicide. The scene where the sexual assault did not take place, but where the offender and the victim were present, is a *secondary crime scene*, relevant for the investigation and collection of evidence. The *intermediate crime scene* is the setting between the main crime scene and disposal site where the evidence or victim was dumped or disposed of. The victim and suspect *medicolegal examination*, involving medical and legal aspects, is of prime importance in establishing what acts did or did not take place. They, together with the statements of the victim, suspect, and the witnesses, put the evidence in perspective and help the investigator reconstruct the crime scene. Reconstruction of the crime scene should consider all evidence, statements, and reports in a sophisticated manner, thereby establishing the truth.

Victim and Suspect Interviews

Interviewing victims and suspects of sexual assault is very different from other crimes. Due to the intimate nature of this type of crime and the taboos and stigmas associated with sex-related crimes, combined with the physical violation alleged to have occurred, severe trauma can result in behavior unlikely to be observed in other heinous crimes. Victims need a degree of comfort and time to speak coherently. They may show odd behavior and may not recall all the events chronologically (Dworkin et al. 2017).

The first issue is to gather as much history of the victim as possible. If the victim reported any crimes previously or belongs to a profession or ethnic group more prone to sexual violence, these can be important indicators to extract information

from the preliminary interviews. As mentioned above, preliminary interviews provide basic information that can be a good starting point, but more interviews are needed as the victim becomes more stable, and the investigator collects more evidence to corroborate the statements of the victim. The basic requirement is to establish trust with the victim. The victim may not be forthcoming due to a variety of reasons. The last thing the investigator wants is to convey a notion to the victim that causes a loss of trust in the investigation. If the victim stops cooperating, the easiest of cases can become very difficult to sustain in the court of law (Chisum and Turvey 2011).

The victims may resort to some lying to protect themselves or people close and dear to them. These lies may not be a big problem if the investigator can put things into context. However, any failure on the part of the investigator to know these issues can jeopardize the trial when such things are brought up by the defense and can easily create doubts on the truthfulness of the crime itself. In short, when the victim is truthful in detailing the actual assault, the case remains solid even if there are some inconsistencies in victim statements throughout the investigation (Searles and Berger 2018).

The time factor should be carefully observed by the investigator. Although it is generally better to interview as early as possible, peculiar circumstances of the case may necessitate a delay of 1 or 2 days. The follow-up interviews and documentation of these interactions should be precise and carefully preserved. The audio recordings, if permissible by law, should be preferred over note-taking or written statements. Interviews should be held in private, as the presence of family, or other individuals, may prevent a victim or offender from being forthcoming. Many questions are not a good strategy as they can confuse the interviewee, but asking the same question repeatedly may help get more information. The interviewer should be prepared to listen and let the interviewee talk. More voluntary information is always better than interrupting the interviewee or sticking to an investigative plan too rigidly. Savino and Turvey (2011, pp. 184–85) recommend a Frame-by-Frame Analysis (FFA) technique where the interviewer focus is on one frame or event at a time. At each frame, the questions try to elicit as much information as possible from the interviewee before moving on to the next subject or time frame. FFA is most useful for victim interviews but can also generate useful information in suspect interviews.

FFA helps significantly in establishing the truthfulness of the grievance and obtaining a confession, despite inconsistencies in the statements. Preliminary interviews can serve as a starting point to structure an FFA-style interview by asking for specific details and time. The exact nature of FFA allows examining the body language of the interviewee for a longer time to gauge truthfulness. Interviewing suspects is different in many aspects. Aside from giving the *Miranda Warning*, which informs the suspect of the right to remain silent, the investigator must have a clear plan for the interview. This preparation enables the investigator to concentrate on key elements and obtain pivotal information needed from the suspect. The investigator should always let suspects tell their side of the story. Once suspects begin talking and telling their side of the story, the investigator should engage in a conversation at key points to arrive at the truth. The investigator must be prepared to fail and have an alternate plan but guard against shutting out the suspect. Nonetheless, the investigator should always avoid obtaining a false confession through pressure or intimidation.

Savino and Turvey (2011) further explain that interviewing children in sexual assault cases can be very challenging. The younger the child, the more likely that he or she would feel intimidated by the investigator. Therefore, the investigator must make an effort to reach the level of the child to make him or her comfortable. However, the investigator should avoid an interview in the presence of parents because the children would often not reveal anything substantial in that situation. Parents often begin answering in place of a child, and the child then believes that every question should be directed to the parents. Likely, a child victim has already been threatened by the perpetrator to remain silent. The investigator should first build a rapport with the children enabling them to feel comfortable and then

commence talking about the incident. The investigator should avoid leading questions, compounding trauma, and asking in judgmental terms. Children have short attention spans and can be easily distracted, of which the investigator needs to be aware. Most importantly, children should be asked if the suspect asked them to remain silent as it can help establish criminal intent. Preteen and teenage male victims are the most difficult to interview as they often believe that talking about the sexual act can label them weak or homosexual.

Victim Management

The victim is the most important link in a sexual assault case. Very often, the victim's body provides important evidence about the suspect as well as the nature and severity of the assault. The victim interview has already been discussed in detail. Therefore, in this section, the emphasis is on the aspects of victim management other than the interview. These aspects can be subdivided into four categories: (1) forensic examination of the victim, (2) eyewitnesses and identification, (3) victim trauma, and (4) false allegations.

Forensic Examination of Victim

The victim's bodily injuries may often provoke the emotions of those investigating, but the investigator should not be affected in objectivity by these emotions. The myths regarding rape victims persist in society. For example, the victims are often blamed for the rape. Sex workers are not believed to be truthful, and provocative clothing is often touted as the reason for rape. Some people think that the victim could have avoided the rape but chose not to do so. That the victim did not fight back is also blamed for the incident. The victim-blaming myths also work conversely. Some victims, including those assaulted by intimate partners, are considered "unrapeable" and hence not believed. These myths have been debunked repeatedly but, unfortunately, persist in every society. An investigator should guard against developing these preconceived notions (World Health Organization 2003).

The recommended approach is to investigate each aspect of the victim separately. Personal details of the victim in general and at the time of an assault are an essential starting point. Physical characteristics and what the victim was wearing or carrying at the time of assault should be recorded diligently. The digital evidence from phones, laptops, and web surfing activities should also be gathered. Victim items and residence should be carefully examined to search and record any clues. Victim personal, intimate, and professional relationships over a long period are important information. The pre-assault financial and medical condition of the victim can reveal curious individuals and helpful information for the investigation. Criminal and legal history should be obtained from the victim as well as other profile sources available to the investigator. The investigator can establish a very comprehensive picture of the victim before the assault and should then proceed to establish the timeline of the actual attack. The victim should always be asked behavioral questions about the offender. The perpetrator's response to resistance, the manner of approach, and any eccentric utterances may help identify the suspect and are important clues that can establish a case against the offender (Savino and Turvey 2011).

Eyewitnesses and Identification

Eyewitnesses, together with the victim story, are an important part of investigations. Lineups and memory lapses can easily identify the wrong suspect if proper care is not undertaken in examining the eyewitnesses. Similarly, show-ups are even more problematic. If the victim was threatened with a weapon, it is natural for a person to focus more on the weapon than the person pointing the weapon. This may later blur the recognition ability of the victim and eyewitnesses. When the victim and eyewitness accounts support the theory built by the investigator, it is straightforward for the investigator to overlook the reliability and credibility of such statements. They may still not constitute "probable cause" and could weaken the case going forward (Savino and Turvey 2011).

Victim Trauma

The victims of sexual assault often experience trauma. They frequently exhibit symptoms of Rape Trauma Syndrome (RTS) and Post Traumatic Stress Disorder (PTSD). Dworkin et al. (2017) argue that the causal relationship between psychopathology and sexual assault cannot be inferred because sexual assault can lead to psychopathology through various mechanisms. For example, sexual assault can make victims more vulnerable to psychological and mental health problems. The victim can have distorted cognition, a state in which the victim overestimates the danger. History of assault can change the mood by increasing fear and sadness in the victim. Sexual assault can also alter the behavior of a person. The victim may feel more socially isolated or get involved in substance abuse. The authors also found that in cases where a weapon was involved, the trauma level was higher, which demands caution against determining the incident to be a causal relationship. The offender often argues that the trauma experienced by the victim somehow led to a false case, especially when nonconsent is the only major argument dividing the two sides. The investigator should, therefore, reject any defense based on the trauma being caused in a causal relationship that does not exist. This precaution does not suggest that if the victim does not exhibit symptoms of trauma, the psychologist's opinion can easily refute the defense argument.

False Allegations

The false allegation of sexual assault is always a possibility, and many investigators are unaware that false reporting is itself a crime. However, even when an investigator is aware and detects a false report, there are social pressures not to reveal the false report. These pressures come from various social organizations, prosecutor offices, and even colleagues because they believe that pursuing such a case is not worth the time and effort, or that type of inquiry goes against the strict guidelines issued by the department to pursue false reports. The reasons for false reporting range from material profit to simple anger and revenge. Sometimes concealment of illicit relations or illegal activity by a domestic partner is the cause behind falsely reporting a sexual assault when none had occurred or was carried out by the intimate partner, which can be embarrassing. In some cases, the false reporter has actual mental issues that result in falsely reporting an assault (Searles and Berger 2018; Chisum and Turvey 2011).

Reconstruction and Physical Evidence

The investigator needs to examine all the evidence and reconstruct the crime scene so that every part of the puzzle falls in its place. Reconstruction is further strengthened by physical evidence obtained through DNA. Sometimes, sexual assaults are facilitated using drugs. These cases require an additional piece of evidence to complete the investigation.

The main elements of crime scene reconstruction, interviews, and crime scene preservation should be established. A forensic examination of the victim is a functional responsibility. World Health Organization (2003) has issued detailed guidelines and procedures to be followed by forensic nurses. An important point in these guidelines notes:

> The physical examination of sexual assault victims must be thorough; it will inevitably be intrusive and time-consuming. In the interest of avoiding multiple examinations and further distress for the patient, the medical examination and forensic evidence collection should, when possible, coincide. Obtaining informed consent for the examination and the release of information to third parties is a crucial component of the service. All parts of the examination should be explained in advance; during the examination, patients should be informed when and where touching will occur and should be given ample opportunity to ask questions. The patient's wishes must be upheld at all times. (World Health Organization 2003, p. 30)

Forensic nurses should also consider the *differential diagnosis*, a diagnosis in which a set of injuries may have more than one cause. The investigator should even document complainant history and toxicology reports. Elements of physical examination, such as injuries, bruises, and full body examination, should also be carefully recorded (Savino and Turvey 2011).

Drug-facilitated sexual assaults are widespread and pose their challenges for the investigators. Apart from common "date-rape" drugs, such as Rohypnol and GHB, other drugs can also be used. Rohypnol is a depressant of the central nervous system. Within 15–30 min of ingestion, the victim starts showing effects that quickly peak in about 2 h and can easily last as long as eight to 12 h. The victim shows dizziness, visual confusion, decreased blood pressure, and drowsiness. GHB decreases inhibitions, thereby stimulating female victims to behave increasingly flirtatiously. Higher doses can lead to sleep and loss of memory. Drug-related assaults differ from other sexual assaults as the victims are rendered unable to consent due to impairment. The victim participation may seem consensual but is manufactured using drugs. The social context and the motives of offenders are also considerably different from traditional assault motives. The investigator should carefully determine whether the elements of occurrence can be considered a sexual assault or rape under statutory definitions. These include whether the victim was actually under the influence to not have consented legally, whether the participation in a sexual act was voluntary or forced by drugs, and whether the offender had access to the drug in question or not (Sexual Assault Prevention and Awareness Center 2018).

DNA technology has radically changed forensic science. Law enforcement has developed CODIS (Combined DNA Index System), which serves as a data bank for DNA matching. DNA match is great news for the investigator, but due care is needed to expand its use. Suspects who are matched may not be actual offenders, especially when DNA is not recovered from the victim's body. Biological evidence can degrade. Therefore, the body should be transported and preserved in a manner that doesn't render it useless as evidence. Semen, sweat, blood, sperm, trace skin, and bodily excretions are conventional sources of DNA. In some cases, such as acquaintance rape, DNA evidence is of no use to the investigator. DNA evidence should be further supported by the conditions of transfer, and other evidence or reconstruction of the crime scene (Chisum and Turvey 2011; Savino and Turvey 2011).

Offender Psychoanalysis

Sexual assault is not purely a crime with sexual motivations only. Offenders can have different motives and may be serial criminals. The motive is different from intent. A motive of revenge may result in different crimes. For example, people rob, kill, or assault in revenge. The intent is the actual action, which translates to a crime. Someone with a motive for revenge will then intend to commit a crime. The motive helps an investigator to put the sexual assault in perspective and boosts the case against the offender. It also helps look at other evidence which may be ignored if the investigator only focuses on the crime itself.

The offender can be divided into different categories based on motive. An *instrumental* offender is motivated by financial or material ends. These offenders are methodical and plan their crimes. On the other hand, the *expressive* offender is motivated by emotions, jealousy, anger, or purely sexual desire (Chisum and Turvey 2011). *Developmental* issues can turn a person towards committing sexual crimes. Beauregard et al. (2004) argue that there are three types of developmental issues: inappropriate family sexual environment, use of pornography and sexually explicit material during childhood, and resulting deviant childhood fantasies about sex. Many other typologies rely on factors other than sexual, such as power or entitlement (Chisum and Turvey 2011, pp. 387–403). While these typologies are helpful tools in assessing the offender, the investigator can often misdirect the effort by solely classifying an offender under one of these categories. Human behavior may change over time, and there may be many other contributing factors, such as mental illness and sexual gratification.

The investigator should pay close attention to the five steps involved in a sexual assault. The offender first selects the target. Once the victim is identified as a target, the offender tests the victim through some implicit sexual advances (if an acquaintance) or analyzes the victim's routine (if a stranger). The offender then threatens the victim and terminates the assault. These acts may happen very quickly or, in some cases, may

unfold over months, all yielding important information about the offender. Some serial offenders use a particular signature or modus operandi. This can connect many offenses to a single perpetrator or previously committed nonsexual crimes to a sexual assault (Savino and Turvey 2011).

Conclusion

Investigation of sexual assault is different from other criminal investigations in many ways. The investigator should not allow preconceived ideas about sexual assault to guide the investigation. The first response is critical as this enables an investigator to record and preserve important physical evidence. Crime scene and DNA evidence should be carefully documented and thorough enough to allow reconstruction of the crime scene. The handling of victims is challenging because of the emotionally traumatic nature of the sexual crime. The investigator's prime source of information is the victim statement and the evidence obtained from the victim's body. The modus operandi of offenders and serial criminals pose their challenges. Specialized knowledge of conducting sex-related crime investigations can significantly help the investigator to arrive at the truth. It is recommended that the investigator take a step-by-step, detailed approach to analyze every aspect of the crime.

Cross-References

- ▶ Workplace: Sexual Harassment
- ▶ Workplace Violence: Sex-Related Crimes

References

Beauregard, E., Lussier, P., & Proulx, J. (2004). An exploration of developmental factors related to deviant sexual preferences among adult rapist. *Sexual Abuse: A Journal of Research and Treatment, 16*(2), 151–161. Also retrieved July 26, 2019, from https://link.springer.com/article/10.1023/B:SEBU.0000023063.94781.bd

Chisum, W., & Turvey, B. E. (2011). *Crime reconstruction* (2nd ed.). San Diego: Elsevier Science. Also retrieved July 26, 2019, from https://books.google.com/books?id=F9JzWnNRyyUC&lpg=PP1&ots=4n636Gb2Yc&dq=Chisum%2C%20W.%2C%20%26%20Turvey%2C%20B.%20E.%20(2011).&lr&pg=PP1#v=onepage&q=Chisum,%20W.,%20&%20Turvey,%20B.%20E.%20(2011).&f=false

Dworkin, E. R., Menon, S. V., Bystrynski, J., & Allen, N. E. (2017). Sexual assault victimization and psychopathology: A review and meta-analysis. *Clinical Psychology Review, 56*(August), 65–81. Also retrieved July 26, 2019, from https://www.researchgate.net/profile/Emily_Dworkin/publication/318062134_Sexual_assault_victimization_and_psychopathology_A_review_and_meta-analysis/links/5b63247d458515298ce0ac10/Sexual-assault-victimization-and-psychopathology-A-review-and-meta-analysis.pdf

Kruttschnitt, C., Kalsbeek, W. D., & House, C. C. (2014). *Estimating the incidence of rape and sexual assault*. National Research Council of the National Academies, Committee on National Statistics Division of Behavioral and Social Sciences and Education. Washington, DC: The National Academies Press. Also retrieved July 26, 2019, from https://www.hoplofobia.info/wp-content/uploads/2014/05/Estimating_the_Incidence_of_Rape_and_Sexual_Assault.pdf

Morgan, R. E., & Kena, G. (2018). *Criminal victimization, 2016: Revised*. Retrieved December 22, 2018, from Bureau of Justice Statistics: https://www.bjs.gov/content/pub/pdf/cv16re.pdf

NFSTC. (2013). *Crime scene investigation: A guide for law enforcement*. Largo: National Forensic Science Technology Center. Retrieved from https://www.nist.gov/sites/default/files/documents/forensics/Crime-Scene-Investigation.pdf

Savino, J. O., & Turvey, B. E. (2011). *Rape investigation handbook* (2nd ed.). Amsterdam: Elsevier. Also retrieved July 26, 2019, from https://books.google.com/books?hl=en&lr=&id=mGaOIzxRByoC&oi=fnd&pg=PP1&dq=Savino,+J.+O.,+%26+Turvey,+B.+E.+(2011&ots=rDmS9quX64&sig=6XSHxZUpzycq2choOJ6UaaBGaRk#v=onepage&q&f=false

Searles, P., & Berger, R. J. (2018). *Rape and society: Readings on the problem of sexual assault*. New York: Routledge.

Sexual Assault Prevention and Awareness Center. (2018). Drugs and sexual assault. University of Michigan. Retrieved from https://sapac.umich.edu/article/51

Silke, A. (2001). *Review of criminal profiling: An introduction to behavioral evidence analysis by Brent Turvey. Crime Prevention & Community Safety, 2001* (3/2), 81–82. Retrieved October 25, 2019 from https://www.academia.edu/13068585/Review_of_Brent_Turvey_Criminal_Profiling_An_Introduction_to_Behavioral_Evidence_Analysis

World Health Organization. (2003). *Guidelines for medico-legal care for victims of sexual violence*. Retrieved December 2018 from http://apps.who.int/iris/bitstream/handle/10665/42788/924154628X.pdf?sequence=1

Further Reading

National Forensic Science Technology Center. (2013). *Crime scene investigation: A guide for law enforcement.* Largo: National Forensic Science Technology Center. Available from https://www.nist.gov/sites/default/files/documents/forensics/Crime-Scene-Investigation.pdf

Savino, J. O., & Turvey, B. E. (2011). *Rape investigation handbook* (2nd ed.). Amsterdam: Elsevier.

Searles, P., & Berger, R. J. (2018). *Rape and society: Readings on the problem of sexual assault*. New York: Routledge.

Silke, A. (2001). Review of criminal profiling: An introduction to behavioral evidence analysis by Brent Turvey. *Crime Prevention & Community Safety, 2001*(3/2), 81–82. Retrieved October 25, 2019 from https://www.academia.edu/13068585/Review_of_Brent_Turvey_Criminal_Profiling_An_Introduction_to_Behavioral_Evidence_Analysis

Investigations: Terrorism

James M. Duggan and James J. F. Forest
Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Keywords

Terrorists · Terrorism · Investigation

Definition

As explained in the ▶ "Criminals: Terrorists" chapter of this volume, terrorists are criminals who commit or directly support acts of violence in order to achieve some type of sociopolitical objectives. An important distinction made in any potential law enforcement investigation is that a "US person" (USPER) is any US citizen or alien granted permanent residency (colloquially known as a "green card").

Introduction

The organizational and operational frameworks within which terrorism investigations are conducted have been significantly enhanced since the attacks of September 11, 2001. Though most will agree that the assorted measures to improve our national security have succeeded in their intent, critics decry the changes as intrusions upon our civil rights and liberties (Chang 2014). Conversely, some may question why the FBI didn't do more in certain instances to protect the USA from harm inflicted by terrorists, just as the FBI bemoans the legal constraints placed upon their tactics and methods to protect the homeland from terrorists. At minimum, the balance between the rights of the individual and the need for a secure homeland was shifted away from civil rights and liberties and toward security in the wake of the attacks of September 11, 2001 (Chang 2014). This chapter will examine some of those changes and leave it to the reader to decide whether the various enhancements went too far, or perhaps not far enough.

Additionally, this chapter will explore the organizational and operational structures that were created or modified since 2001, as well as the legislation and FBI policy and procedures that drive the investigation of terrorists by US law enforcement. Although local and tribal officers are certainly capable and not prohibited from conducting terrorism investigations, only federal agents and duly authorized task force officers (TFOs) may make applications to the Foreign Intelligence Surveillance Court, and the established framework for terrorism investigations suggests that those investigations should be conducted by the FBI's Joint Terrorism Task Forces (JTTFs), in which state, local, and tribal officers participate as TFOs (ODNI fact sheet). This chapter will therefore focus on terrorism investigations conducted within the framework established by the federal government.

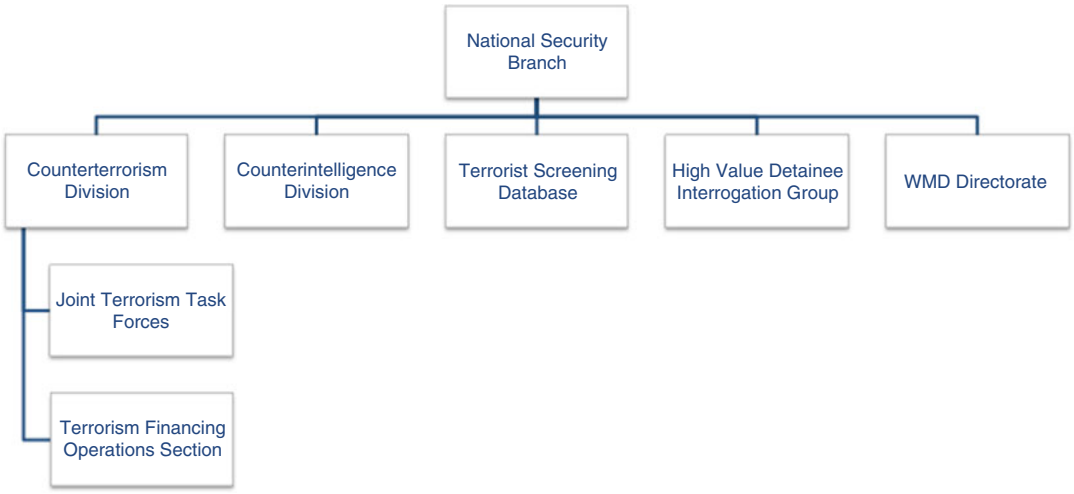
Organizational Structure

The Department of Justice (DOJ) encompasses numerous agencies and divisions that contribute to the US government's efforts to investigate terrorist-related offenses. The DOJ's National Security Division was established in 2006 with the passage of the USA PATRIOT Reauthorization and Improvement Act and tasked with the primary responsibility of combating terrorism (FBI NSD). The National

Security Division coordinates the collective counterterrorism enforcement efforts of their subordinate agencies and others, including the various US Attorneys' Offices, the National Security Branch of the FBI, and the various agencies of the collective US intelligence community (IC), which are discussed in the ▶ "Intelligence" chapter within this volume (FBI NSD). In addition, the National Security Division provides guidance to prosecutors relative to the use of classified information in the criminal prosecution of individuals charged with terrorist offenses and leads DOJ efforts to counter terrorist financing and money laundering (FBI NSD).

The FBI is a vital component of the DOJ and is subordinate to the NSD. The primary responsibility of the FBI is to protect the USA from terrorist threats (USA PATRIOT Act). Per order of a Presidential directive, the FBI established their National Security Branch (NSB) in 2005 to organize the Bureau's national security assets under one umbrella (FBI NSD). The NSB is comprised of five groups and divisions which are disaggregated by area of expertise, allowing the FBI to appropriately assign cases after determining if the subject of investigation is primarily an intelligence or criminal matter (FBI NSD). As discussed in the ▶ "Criminals: Terrorists" chapter within this volume, the lines between terrorists and criminals have become increasingly blurred as terrorist organizations turn to crime to fund their operations and collaborate with criminal groups for incident-specific assistance such as document forgery, smuggling weapons or personnel, and other forms of logistical support (Forest 2013).

The NSB organizational unit (see Fig. 1) most narrowly focused on investigations of terrorism is the Counterterrorism Division (CTD), which oversees the Joint Terrorism Task Forces (JTTFs) and Terrorism Financing Operations Section (TFOS). The FBI's JTTFs are the primary mechanism for investigating terrorist activity within the USA and are comprised of special agents from 55 federal law enforcement agencies as well as state, local, and tribal officers (FBI JTTF). Each JTTF aims to identify and disrupt terrorist threats (FBI JTTF), whether by arrest, administrative actions available to the many agencies involved in the JTTF, or other creative solutions such as the facilitation of mental health treatment. To develop a criminal investigation and collect the requisite evidence while simultaneously managing the threat posed by aspiring terrorists is a daunting task that most often results in a quiet disruption by means other than an arrest. There are currently 104 JTTFs nationwide, 71 of which have been established since the attacks of September 11, 2001 (FBI JTTF). The TFOS



Investigations: Terrorism, Fig. 1 Components of the FBI National Security Division most narrowly focused on terrorism investigations

collaborates with the IC and global partners to identify, investigate, disrupt, and dismantle terrorist financing and money laundering networks throughout the world (FBI NSD).

Other components of the NSB are the Counterintelligence Division (CID), the High-Value Detainee Interrogation Group (HIG), the Terrorist Screening Center, and the Weapons of Mass Destruction (WMD) Directorate. The CID investigates the espionage activities of foreign governments (adversaries as well as allies) and their representatives to identify and disrupt their efforts to steal intellectual property from the US government, businesses, and universities (FBI NSD). Stolen trade secrets and intelligence present opportunities for hostile actors, including terrorists, to develop weapons and technologies that may be used in attacks against Americans in the USA and abroad (FBI NSD). Cyber intrusions have become an especially appealing mechanism to steal intelligence and trade secrets and have therefore become a primary focus of CID (FBI NSD), in collaboration with the National Security Agency (NSA) (Sinai 2014).

The HIG is administered by the FBI and is comprised of special agents, linguists, subject matter experts, and interrogators from various IC agencies that are deployed to conduct effective interviews of high-value detainees in a manner that is consistent with the rule of law (FBI NSD). HIG personnel consistently collaborate with researchers from academia to stay abreast of the latest, most effective interview techniques, as well as to contribute to research on interview techniques (FBI NSD). The HIG deploys Mobile Interrogation Teams to the field during emergent situations and may be used to collect intelligence as well as evidence to be used in a criminal prosecution (FBI NSD).

The Terrorist Screening Center is another multi-agency effort that is administered by the FBI and manages the Terrorist Screening Database, colloquially known as "The Watchlist" (FBI NSD). The Terrorist Screening Database provides an effective early warning detection system at ports of entry and during the processing of visas by the Department of State by compiling and managing a single list of subjects that the government has determined are, or have an association to, known or suspected terrorists at the level of reasonable suspicion (FBI NSD). The Terrorist Screening Database essentially provides a one-stop shopping list of known and suspected terrorists for law enforcement.

The WMD Directorate is the fifth component of the FBI's National Security Branch. The WMD Directorate was established in 2006 and is tasked with proactively preventing chemical, biological, radiological, and nuclear (CBRN) materials and weapons from entering the USA, to identify and disrupt the intended deployment of CBRN materials and weapons, and to respond to incidents involving CBRN materials (FBI NSD). In addition, the WMD Directorate is responsible for establishing and managing "tripwires," which are a staple of our national security and conducted via education and collaboration with private industry, academia, and public health organizations to identify suspicious inquiries or purchases of materials indicative of the collection of materials, knowledge, or expertise necessary to launch an attack (FBI NSD).

Operational Framework

National SAR Initiative

The National Strategy for Information Sharing was enacted by President George W. Bush in 2007 to standardize the collection, handling, and dissemination of suspicious activity reports (SARs) to maximize the utility of the reports and assure that civil rights and rights to privacy are adhered to (ODNI fact sheet). A primary component of the National Strategy for Information Sharing is the National SAR Initiative (NSI). Incidents and behavior reasonably believed to be consistent with international or domestic terrorism justify the documentation of a SAR (ODNI fact sheet). The NSI establishes roles and responsibilities, as well as workflows, for the collection, handling, and dissemination of SARs among the various federal agencies, as well as state, local, and tribal agencies (ODNI fact sheet). Suspicious activity reporting involves one or more of the 79 fusion centers located throughout the USA. These fusion centers are primarily staffed and managed by state police agencies, but many

Incident, Behavior of Concern Reported to Fusion Center
Suspicious Activity Report
Information Sharing Environment
Joint Terrorism Task Force

Investigations: Terrorism, Fig. 2 National SAR Initiative reporting process

also incorporate embedded FBI (FBI JTTF) and Department of Homeland Security intelligence analysts that are provided initial visibility of, and the opportunity to contribute to, the SAR. The standardized procedures require that these fusion centers collect SARs from the public and local law enforcement, as well as private industry partners, most important of which are those responsible for critical infrastructure and key resources (ODNI fact sheet). Law enforcement professionals assigned to the fusion center then examine the reported activity to determine if it meets the SAR standards and if so, document the reported incident or behavior as a SAR (ODNI fact sheet). The completed SAR is then disseminated to the appropriate federal, state, and local agencies (see Fig. 2) via the "Information Sharing Environment" (ISE) that is provided by the FBI's Internet-based eGuardian portal that is available to law enforcement agencies across the country (ODNI fact sheet). The ISE makes the SAR available to other agencies for their situational awareness and reviewed by the FBI's Counterterrorism Division for final determination of whether the reported activity or behavior fits SAR criteria. If deemed a fit with established criteria, the SAR is then assigned via Guardian (classified version of eGuardian) to the appropriate JTTF for investigation. Various laws and policies intended to assure adherence to privacy and constitutional rights throughout the established process are incorporated into the NSI (ODNI fact sheet).

Legislation, Policy, and Procedures

Foreign Intelligence and Surveillance Act (FISA) of 1978

The FISA of 1978 was passed by Congress in response to the revelation that the FBI had been employing wiretap and other electronic surveillance technologies domestically against USPERs for decades (Golden 2014) under the guise of national security. FISA established guidelines and protocols to assure judicial oversight by the Foreign Intelligence and Surveillance Court for the employment of such technologies by federal law enforcement against USPERs (Golden 2014). Among the limits established by FISA were that the target of the surveillance must be either a foreign power or the agent of a foreign power and "that no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States" (FISA 1978, p. 9).

USA PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (PATRIOT Act) was a direct response to the attacks of September 11, 2001, and shifted the focus away from protecting civil rights, which had been established by FISA, and toward a prioritization of national security (Chang 2014). Proponents of the PATRIOT Act contend that, among other things, the Act makes the country safer by streamlining the legal processes required for judicial approval and allowing for a speedier response by law enforcement to emergent threats while still providing for effective oversight (Hook et al. 2014). Some examples of the changes introduced by the PATRIOT Act (2001) that contribute to law enforcement efforts are roving wiretaps, national wiretap authorization, "sneak-and-peek" search warrants (notice of a search is not provided to the subject), and a change from the requirement that collection of foreign intelligence is "the purpose" of a search or wiretap to the less stringent standard of "a significant purpose" (Chang 2014). Among the arguments offered by opponents

of the PATRIOT Act are that the allowance of sneak-and-peek searches is an intrusion on a tenet of the 4th amendment requiring that law enforcement "knock and announce" their presence prior to entering a place to be searched (Chang 2014).

In the aftermath of the September 11, 2001, attacks, the US government took significant strides to combat terrorist financing and money laundering. Title III of the PATRIOT Act established the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 which significantly enhanced the ability of the USA to prevent, detect, and disrupt (by civil forfeiture or criminal prosecution) the flow of illicit funds through US-based institutions (USA PATRIOT Act 2001). Title III prohibits US-based bank accounts from conducting transactions with offshore "shell" banks that did not have a physical address and strengthened the previous Bank Secrecy Act by requiring additional due diligence by banks (USA PATRIOT Act 2001). Due diligence enhancements include confirming the identity of all foreign nationals associated with an account and proactive monitoring of accounts held by foreign nationals or organizations for indications of terrorist financing or money laundering (USA PATRIOT Act 2001).

Policies and Procedures

In addition to legislation regulating the domestic investigative activities of US law enforcement, there are also institutional policies and regulations that must be adhered to. The domestic investigative efforts of the FBI are tightly regulated by the 457-page *Domestic Investigation and Operations Guide* (DIOG), which incorporates guidelines established by the US Attorney General and FBI policies and procedures into a single manual (Federal Bureau of Investigation 2016). The FBI is limited by the DIOG to assure that the least intrusive methods possible are employed at various stages of an investigation, and unless articulable evidence is developed at the earlier stages of a case to justify further investigation with more invasive methods (Federal Bureau of Investigation 2016), the case will be either closed or prosecuted in its current state. Unfortunately, the subjects of closed cases sometimes commit violence, such as Tamerlan Tsarnaev (2013 Boston Marathon bombing) and Omar Mateen (2016 Pulse Nightclub, Orlando attack). As for Mateen, the FBI staunchly defended their prior 10-month investigation of Mateen, insisting they exhausted all legal means of investigation before determining Mateen posed no articulable threat to the public and closing the case (Wilbur 2016).

Though the DIOG may frustrate the good intentions of law enforcement at times, it is necessary for the government to assure that the law and public policy appropriately balance the rights of the individual with the need for national security (USA PATRIOT Act). Closed cases that go awry and result in harm are not necessarily mistakes but may rather be symptomatic of the FBI's adherence to the DIOG, which maintains core values of the USA by favoring the preservation of individual rights over national security. And of course, there is no infallible way to predict what an individual may or may not do in the future.

Characteristics of Terrorism Investigations

The very nature of terrorism necessitates clear distinctions between domestic and international terrorism and the permissible methods to be employed against each (further details of the distinctions between the two can be found in the ▶ "Terrorism: Domestic" and ▶ "Terrorism: International" chapters within this volume). Because terrorism is a form of political violence, domestic issues must be treated carefully to assure that political dissidents are not unfairly targeted (Chang 2014). The *Immigration and Nationality Act* established that the Secretary of State shall compile and maintain the list of designated foreign terrorist organizations (FTOs). To knowingly provide material support to a designated FTO is a criminal offense, but there is no such provision relative to domestic terrorist organizations (USA PATRIOT Act 2001).

For example, in 2006 the FBI indicted 11 members of the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF) that had formed an organization known as "the Family," one of the most prolific domestic terrorist organizations in the history of the USA (Federal Bureau of Investigation, *Eco-terror indictments*). The group conducted a campaign of bombings and arsons that included the Vail Ski Resort, federal land and animal management facilities, private meat-processing plants, and logging operations (Federal Bureau of Investigation, *Eco-terror indictments*). Because the Family was a domestic terrorist organization, they were charged with crimes committed in support of the Family, but there was no specific charge for providing material support to the Family.

As stated previously, many of the cases investigated by the JTTF are predicated upon suspicious activity that was reported to law enforcement. However, although possibly indicative of current or pending terrorist activity, the overwhelming majority of suspicious behaviors and actions that provide the basis for SARs are not illegal (ODNI fact sheet). For instance, it is not illegal to purchase a large amount of fertilizer for no obviously legal purpose. However, such a purchase would likely trigger a "tripwire" established by the FBI's WMD Directorate, generation of a SAR, and assignment to the most appropriate JTTF for investigation at the most appropriate level, most often an assessment (Federal Bureau of Investigation 2016). The inherent difficulty of terrorism investigations is that the JTTF member assigned to investigate the incident does not have the benefit of investigating a past crime, but rather must determine if the suspicious purchase is an indicator of a crime (terrorist attack) to be committed in the future, based largely upon constitutionally protected behaviors and speech.

There have been criticisms of FBI methods and target selection of individuals who have been convicted of terrorism-related offenses. The general basis of the assertion is that defendants who had neither the ability nor means to carry out an attack were "entrapped" by FBI informants and undercover agents who hatched a plot and provided the materials necessary to justify a federal prosecution (Shipler 2012). It is sometimes asserted that the defendant could not have ever collected the requisite weapons or materials without the assistance of the government (Crenshaw and LaFree 2017). However, appeals courts have repeatedly denied these claims of entrapment and violation of due process by defendants, finding that defendants were predisposed to commit the crime and that "…government creation of the opportunity to commit an offense, even to the point of supplying defendants with materials essential to commit crimes, does not exceed due process limits" (United States of America v. Cromitie, p. 57).

Despite the firm legal ground that these counterterrorism investigations may be based upon, judges presiding over trials and appeals have at times expressed concern with the targeting and tactics employed by law enforcement. In sentencing James Cromitie to 25 years in prison for assorted terrorism charges, federal district court judge Colleen McMahon proclaimed that "Only the government could have made a 'terrorist' out of Mr. Cromitie, whose buffoonery is positively Shakespearean in its scope" (Shipler 2012). However, in denying the appeal of Cromitie et al., Circuit Judge Jon O. Newman of the Second Circuit Court of Appeals explained in the majority opinion that once Cromitie had "…expressed a desire to 'do something to America' and had given an ominous meaning to this statement by saying he wanted to die like a martyr, the FBI agents would have been derelict in their duties if they did not test how far Cromitie would go to carry out his desires" (United States of America v. Cromitie, p. 57). Additionally, as noted by Crenshaw and LaFree (2017), many individuals who have carried out successful attacks also seemed to lack the skills and tradecraft necessary to do so, which is especially cogent in an era of attacks with crude weapons such as knives and automobiles driven into crowds of innocent civilians.

Case Studies

Further evidence of the quandary presented by terrorism investigations can be found in case

studies of JTTF investigations. Even as judges periodically express concern with methods employed in some investigations, they also cite the duty of the FBI to investigate those individuals who indicate their desire to cause harm (United States of America v. Cromitie). Most proactive criminal investigations target individuals who are already involved in the prohibited activity, such as drug dealers or arms traffickers, but proactive terrorism investigations require the targeting of individuals and groups who may commit a crime in the future (Shipler 2012). Thankfully, there is a dearth of active terrorist operatives on American streets, leaving investigators to target those who display a risk of attacking in the future (Shipler 2012). The cases targeting James Cromitie and Demetrius Pitts are illustrative of the controversies and difficulties associated with terrorism investigations.

Example 1: USA v. James Cromitie, David Williams, Onta Williams, and Laguerre Payen
The following details of the case of the USA v. James Cromitie, David Williams, Onta Williams, and Laguerre Payen were gleaned from an affidavit submitted by the FBI to the Southern District of New York on May 19, 2009, in support of an application for arrest warrants for Cromitie et al. (Fuller 2009).

In June 2008, James Cromitie, the son of Afghan immigrants, expressed his dismay with US military actions in Afghanistan to a paid FBI informant (CHS – confidential human source) that Cromitie met at a mosque in Newburgh, New York. Cromitie further expressed his desire to do "something to America" and discussed with the CHS how Cromitie would go to paradise if he died a martyr. The two met again on July 3, 2008, and the CHS told Cromitie that the CHS was a member of Jaish-e-Mohammed, a designated FTO based in Pakistan, to which Cromitie responded that he would like to "do jihad" (p. 6). Cromitie recruited three friends (David Williams, Onta Williams, and Laguerre Payen) who began meeting with Cromitie and the CHS at a house in Newburgh that had been outfitted by the FBI with audio and video surveillance equipment. Discussion at the house revolved around Cromitie's desire to attack a synagogue in the Bronx and military aircraft based at the Air National Guard base in Newburgh.

In a recorded conversation on December 5, 2008, Cromitie asked the CHS to get surface-to-air missiles, rockets, or other explosives for Cromitie's future operations and explained to the CHS that they would need to develop code words for future conversations. In April 2009, the CHS, Cromitie, and Williams drove to the Bronx and drove by several synagogues and Jewish community centers, which Cromitie specified would be referred to as "joints" in future discussions. In addition, Cromitie drew attention to a group of people walking outside a Jewish community center and said that if he had a gun, he would shoot each one in the head.

On April 23, 2009, the CHS met with Cromitie and Williams at the Newburgh house where they discussed using surface-to-air missiles to attack aircraft at the Air National Guard base and improvised explosive devices (IEDs) to attack a synagogue. They further discussed code words, as well as the need for cell phones and handguns, which Williams arranged the purchase of with a female gun supplier in the Newburgh area. The CHS coordinated with individuals (believed by Cromitie and the others to be members of Jaish-e-Mohammed) to supply one Stinger missile and three IEDs constructed with c4 explosives and advised Cromitie and the others of the arrangement.

After conducting surveillance of the Air National Guard base and determining the location from which to fire the missiles, Cromitie and Williams engaged in a telephone conversation that was intercepted (the inference is via a court-authorized wiretap of at least one of the devices used for the conversation) in which Williams advised Cromitie that Williams had procured the handguns. However, when the group drove to retrieve the guns, the supplier said she had sold them to someone else. The group then picked up Onta Williams (whom David Williams had recruited to assist with the attacks), bought cell phones for the operation, and after numerous phone calls was able to arrange for the purchase of a handgun.

On April 28, 2009, the group was joined by Laguerre Payen in the Newburgh house and engaged in recorded conversation, in which all declared their willingness to engage in the planned attacks in support of Jaish-e-Mohammed. Onta Williams stated that "they [the United States military] are killing Muslim brothers and sisters in Muslim countries so, if we kill them here [in the United States] with IEDs and Stingers, it is equal" (pp. 10–11). The group then drove toward a storage facility in Connecticut to retrieve the Stinger missile and three IEDs, but Onta Williams thought he detected law enforcement surveilling the group so they returned to Newburgh. Onta Williams was dropped off in Newburgh, and after driving and determining that law enforcement was no longer following them, they drove to Connecticut and retrieved the missile and explosives before returning to Newburgh, where the payload was stowed in a storage facility. All of the defendants inspected the missile and explosives, before practicing with the remote detonator for the IEDs and exclaiming "Allahu Akbar" (praise be to God) as they locked the door to the storage unit. On May 19, 2009, the FBI applied for and was granted arrest warrants from a US Magistrate Judge in the Southern District of New York charging all four co-conspirators with conspiracy to use weapons of mass destruction within the USA, conspiracy to acquire and use antiaircraft missiles, and conspiracy to kill officers and employees of the USA.

All four were convicted and sentenced to 25 years in prison. The case was appealed to the US Court of Appeals for the Second Circuit in 2012 and denied, with one justice concurring with Cromitie's claim of entrapment (United States of America v. Cromitie). However, the two other justices denied all claims made by the defendants, and the sentences of all four were therefore upheld. In their majority opinion, the justices stated, "the principal defendant expressed early on an inclination to commit acts of terrorism and his co-defendants promptly and enthusiastically joined the plot with full awareness that it included launching anti-aircraft missiles. The Government did nothing improper by testing to see just how far these defendants would go in committing acts of terrorism" (United States of America v. Cromitie, p. 77).

Example 2: USA v. Demetrius Pitts

The facts of the FBI's case against Demetrius Pitts were culled from an FBI affidavit filed in support of a criminal complaint charging Pitts with one count of material support to a FTO (Wilson, A.J., United States of America v. Demetrius Pitts). Unlike the previous case, Pitts has not been convicted, but stands accused of the crime with which he is charged, and remains innocent until proven guilty. The Pitts case is illustrative of a typical JTTF investigation predicated upon a SAR.

On July 1, 2018, Demetrius Pitts of Maple Heights, Ohio, was arrested and charged with attempting to provide material support or resources to a foreign terrorist organization in violation of Title 18, United States Code, Section 2339B. Pitts originally came to the attention of the FBI in December 31, 2015, when he sent a private Facebook message to a political television show expressing his contempt for the USA in general as well as the US military, more specifically, and further stated that the USA would be destroyed. The incident was reported by representatives of the television show, which generated a SAR to be investigated (the inference is as an assessment). Legal process served upon Facebook by the US Attorney's Office for the account revealed that Pitts was the user of the account and utilized a pseudonym for the Facebook account.

Pitts did not come to the attention of the FBI again until January 2017, and it is unclear what investigative activities were undertaken in the interim, if any. On January 25, 2017, Pitts commented on images of activities in an al-Qaeda training camp via Facebook, opining that Muslims should be learning how to shoot guns and training every day. Pitts posted, "If you fear death. Then you don't love Islam. . .we should always be prepared to fight in the name of Allah Akbar" (p. 3). Between January 25, 2017 and June 2018, Pitts continued with violent rhetoric via Facebook, which evolved into Pitts expressing his desire to travel overseas to receive training

for an attack to be launched in the USA. In addition, Pitts expressed his aspiration for recruiting others to join him in future attacks within the USA. When Pitts disclosed his desire to meet a "brother" from al-Qaeda, the FBI obliged by assigning an undercover special agent (UCE – undercover employee) to make contact with Pitts and present themselves as an al-Qaeda operative.

On June 15, 2018, Pitts met with the UCE, who conducted a "consensual recording" of the meeting. It is worth noting that Pitts obviously did not consent to the recording, but federal law permits one-party consent, meaning only one individual involved in the recording must consent to that recording. Just as a co-conspirator working on behalf of the government may consent to recording a conversation with the subject of an investigation, the UCE provides the consent in an undercover operation.

In recorded conversation with the UCE, Pitts explained that he wanted to target members of the military, cut off their head and hands, and anonymously mail them to government officials to "make a statement." When the UCE inquired about targeting sporting events and stadiums, Pitts explained that it would be best to target military members who had engaged in combat with Muslims rather than innocent civilians, stating that "These people ain't got nothing to do with it" (p. 5). Pitts acknowledged to the UCE that the brothers may want Pitts to prove himself before they agree to collaborate with him and was clear that he was willing to kill a military member, stating "That's what they signed up for. Look at they signed up for war. Guess what? They want war, we can bring war to them" (p. 8).

One week later, on June 22, 2018, the two met and engaged in another recorded conversation in which Pitts conveyed his interest in launching an attack on the 4th of July. Pitts considered attacking an event in Washington DC but quickly decided there would be too much security and then discussed attacking a parade and fireworks display in downtown Cleveland, Ohio. Pitts suggested they could employ small remote-controlled cars outfitted with bombs to attack the parade. Pitts requested that the UCE get money from the brothers to fund his trip from the Cleveland suburbs to the downtown area so that he may conduct reconnaissance and take photographs and video for the brothers.

On June 25, Pitts met with a CHS posing as an al-Qaeda member who provided Pitts with a bus ticket and a phone to be utilized in his reconnaissance efforts. On June 26, members of the FBI Cleveland JTTF conducted physical surveillance of Pitts as he toured downtown Cleveland, taking photographs and video of potential targets. Pitts contacted the UCE via text message with an update of his activities and began discussing an attack in Philadelphia, telling the UCE that the brother who was making the bombs for Cleveland should continue but they would need more for Philadelphia. Pitts explained to the UCE that he would identify the targets but other brothers would have to conduct the attacks and gave the phone used for the pre-operational surveillance of Cleveland to the UCE, with Pitts' password of "0704."

Later in the day on June 27, Pitts met with the UCE and disclosed that he thought a van loaded with explosives would be the best opportunity for success to target US Marines marching in the 4th of July parade. Pitts reiterated that he would conduct the pre-operational surveillance and the brothers must handle the explosives, but Pitts didn't want to meet the brothers to be involved in the attack for operational security reasons. Pitts provided the UCE with his personal phone that he had also used for pre-operational surveillance and advised the UCE that he would like to be called "Salah ad-Deen," which is Arabic for "the planner." Search warrants executed on the phones revealed two videos of Pitts pledging allegiance or "bayah" to al-Qaeda, as well as photographs and video taken by Pitts. While driving together the UCE and Pitts passed the US Coast Guard base in Cleveland, and Pitts decided the explosives-laden van should be parked immediately adjacent to the Coast Guard building and detonated as US Marines marched past.

The investigation culminated in a July 1, 2018, meeting between Pitts and the UCE in which Pitts pitched his plan for a future attack against the Federal Building in Philadelphia that Pitts felt would "hit 'em in the gut" (p. 29). When the UCE commented that there would be "human carnage"

and "that body parts would be flying around," Pitts explained that he wouldn't have any remorse and wouldn't lose any sleep over the incident. When the UCE showed Pitts a c4-laden remote-controlled car that the purported al-Qaeda bombmaker made for their operation, Pitts suggested they replace the BBs packed with the explosives with cut-up pieces of metal because it is possible to survive the BBs but that shrapnel would "tear you up" (p. 29).

Pitts further suggested that they give the cars to the children of military members as gifts, in the hopes that they would detonate the cars at home. Pitts was then arrested pursuant to a criminal complaint issued by US Magistrate Judge David Ruiz and charged with attempting to provide material support or resources to an FTO. On July 25, 2018, Pitts' public defender advised the court that Pitts has a long history of mental illness and requested a mental health evaluation, a move which was not objected to by federal prosecutors. Magistrate Judge David Ruiz ordered the evaluation (results of which are pending) and explained that the next hearing would be subsequent to the release of the mental health evaluation (Heisig 2018).

Conclusion

Identifying the appropriate balance between civil liberties and national security is a delicate subject that evokes passion on both sides of the argument, and appropriately so, as this strikes at the most fundamental tenets of our democracy. The enhanced tools for law enforcement that were provided through legislation passed since 2001(especially the PATRIOT Act) are alleged by some to have strengthened national security at the expense of liberty (Chang 2014). Conversely, law enforcement is often frustrated by restrictions of allowable methods placed upon them by the DIOG (Wilbur 2016), which is exacerbated by the public's unrealistic expectation of complete immunity from terrorist attack. The fulcrum has shifted throughout time and will continue to do so, as the context of the time and public pressure of the electorate influences political decision-making.

The investigations of Cromitie and Pitts illustrate many of the issues inherent in terrorism investigations. Were Cromitie and Pitts "buffoons" or future terrorists that were appropriately identified and investigated with great diligence by the JTTF before having their plots disrupted by arrest before they could cause harm? Investigation of terrorists requires great skill and judgment, as law enforcement must navigate the laws and policies intended to protect us from unwanted law enforcement intrusions into our daily lives as they tirelessly pursue those who intend to do us harm.

Cross-References

- ▶ Criminals: Terrorists
- ▶ Terrorism: Domestic
- ▶ Terrorism: International

References

Chang, N. (2014). The USA PATRIOT Act: What's so patriotic about trampling on the Bill of Rights? In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism* (2nd ed.). New York: McGraw-Hill.

Crenshaw, M., & LaFree, G. (2017). *Countering terrorism*. Washington, DC: The Brookings Institution.

Federal Bureau of Investigation. (2016). *Domestic investigations and operations guide*. Washington, DC: U.S. Government Printing Office. Retrieved from https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view

Federal Bureau of Investigation. Eco-terror indictments: 'Operation Backfire' nets 11. Retrieved from https://archives.fbi.gov/archives/news/stories/2006/january/elf012006

Federal Bureau of Investigation (FBI), National Security Branch (NSB). Retrieved from https://www.fbi.gov/about/leadership-and-structure/national-security-branch

Foreign Intelligence Surveillance Act of 1978. (1978). Pub. L. no. 95–511, 92 Stat. 1783

Forest, J. J. F. (2013). *Intersections of crime and terror*. New York: Routledge.

Fuller, R., United States of America v. Cromitie, D. Williams, O. Willams, & Payen (Affidavit for Arrest

Warrants), May 9, 2009. Retrieved from https://www.investigativeproject.org/documents/case_docs/952.pdf
Golden, R. D. (2014). What price security? The USA PATRIOT Act and America's balance between freedom and security. In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism* (2nd ed.). New York: McGraw-Hill.
Heisig, E. (2018). Lawyer for suspect in Cleveland Fourth of July terrorism plot seeks competency evaluation for client. Cleveland.com. Retrieved from https://www.cleveland.com/court-justice/index.ssf/2018/07/lawyer_for_cleveland_terrorism.html
Hook, B. H., Peterlin, M. J. A., & Welsh, P. L. (2014). The USA PATRIOT Act and information sharing between the intelligence and law enforcement communities. In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism* (2nd ed.). New York: McGraw-Hill.
Shipler, D. K. (2012). Terrorist Plots, Hatched by the F.B.I. *New York Times*. Retrieved from https://www.nytimes.com/2012/04/29/opinion/sunday/terrorist-plots-helped-along-by-the-fbi.html
Sinai, J. (2014). Najibullah Zazi's plot to bomb the New York City subway system. In J. J. F. Forest, R. D. Howard, & J. C. Moore (Eds.), *Homeland security and terrorism* (2nd ed.). New York: McGraw-Hill.
United States of America v. Cromitie (Williams), 727 F.3d 194 (6th Cir., 2012). Retrieved from https://cases.justia.com/federal/appellate-courts/ca2/11-2763/11-2763-2013-08-23.pdf?ts=1410918996
United States Office of the Director of National Intelligence (ODNI), Fact sheet: Update to suspicious activity reporting functional standard provides greater privacy and civil liberties protections (May 21, 2009). Retrieved from https://www.dni.gov/files/ISE/documents/DocumentLibrary/SAR/ISE-SAR_Functional_Standard_V1_5_Fact_Sheet.pdf
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 109-58, 115 Stat. 272 (2001).
Wilbur, D. Q. (2016). The FBI investigated the Orlando mass shooter for 10 months – And found nothing. Here's why. *Los Angeles Times*. Retrieved from http://www.latimes.com/nation/la-na-fbi-investigation-mateen-20160712-snap-story.html
Wilson, A. J., United States of America v. Demetrius Pitts (affidavit), July 2, 2018. Retrieved from https://assets.documentcloud.org/documents/4569149/PITTSaffidavitforcomplaint.pdf

Further Reading

Crenshaw, M., & LaFree, G. (2017). *Countering terrorism*. Washington, DC: The Brookings Institution.
Federal Bureau of Investigation. (2016). *Domestic investigations and operations guide*. Washington, DC: U.S. Government Printing Office.
Forest, J. J. F. (2015). *Essentials of counterterrorism*. Westport: Praeger Security International.

Investigations: Use of DNA and Fingerprints

Brian Kohlhepp
John Jay College of Criminal Justice, New York, NY, USA
Detective Sergeant, Ross Township Police, Pittsburgh, PA, USA

Keywords
Fingerprints · Palm print footprint · AFIS · IAFIS · Identification · Friction ridge · Deoxyribonucleic acid · Semen · Blood · Saliva · Epithelial cells · CODIS · Identification · Robbery · Burglary · Rape · Sex assault · Murder · Homicide · Interview · Interrogation · Evidence · Crime scene · Trial · Prosecution

Definition

Fingerprint evidence comprises of the study and comparison of the friction ridge detail that is present on one's fingers, as well as the palms of their hands, soles of their feet, and toes. During daily activity, we leave behind impressions of these friction ridges either through sweat and other material on our hands or contact with a foreign substance such as blood or grease and then touching a clean surface leaving a tracing of friction ridges. These can be collected by crime scene personnel and compared to the friction ridges of known persons or prints collected at other crime scenes in an attempt to determine who contributed these prints. This then confirms to the investigator that this person had to have been present and/or touched this object. In this practice, genetic material is used to answer questions pertaining to the investigation. Often during the course of our daily activity, we leave behind genetic material. This is as simple as remnants of saliva on coffee cups and water bottles, to skin cells on the clothing we wear and items we hold. There are specific types of activity, of which the criminality may be in

question that are more likely to produce and dispose of genetic material. This is most common with sex-related activity and death investigations. These can be collected by crime scene personnel and compared to the friction ridges of known persons or prints collected at other crime scenes in an attempt to determine who contributed these prints. This then confirms to the investigator that this person had to have been present as well as generally how they interacted at the scene. Saliva on a cup would indicate that the person drank from that cup, while semen in a sex assault victim's vagina indicates sexual activity.

Introduction

Fingerprint evidence is one of the best and most probative of all types of physical evidence. It can be used to identify people as well as associate them with locations or objects. It should be sought at crime scenes, especially scenes with unknown perpetrators (James et al. 2014). The forensic science discipline which had made the most strides and gained the most attention in the recent past is that of forensic biology, which is comprised of the disciplines of body fluid identification/serology and DNA analysis. This area can be of great value to investigators and provide information that is both relative and substantial in its investigative and evidentiary value.

Fingerprint

Fingerprint evidence is one of the best and most probative of all types of physical evidence. It can be used to identify people as well as associate them with locations or objects. It should be sought at crime scenes, especially scenes with unknown perpetrators (James et al. 2014).

While still in the womb, the friction ridges are formed and the arrangement of the ridges does not change through one's lifetime. Friction ridge skin is composed of two layers of skin. The outermost layer is known as the epidermis and the innermost layer is known as the dermis. The "blueprint" for an individual's friction ridge skin is rooted in the bottom layer of the epidermis, called the basal layer. As long there is no trauma to the basal layer, an individual's friction ridge skin arrangement will not change. In fact, even if one burns off the top layers of the epidermis with an acid, they will grow back in exactly the same fashion. The only way a fingerprint can be changed is through a traumatic event of the basal layer. Trauma to the basal layer will result in a permanent scar. However, the ridges around the area of trauma will remain the same.

Fingerprint evidence comprises of the study and comparison of the friction ridge detail that is present on one's fingers, as well as the palms of their hands, soles of their feet, and toes. As the name of the discipline implies, the vast majority of this work focuses on the friction ridges on the end of one's fingers. This is the volar skin, and it has a special texturized surface with narrow corrugated ridges, known as friction ridges. They are meant to increase our ability to grip other surfaces with which they come into contact. "Smooth skin contains hair, sebaceous glands and sweat glands while volar skin contains only sweat glands" (Ashbaugh 1999). Latent prints are made when sweat from the volar skin as well as the oils from the subject's face, hair, or other parts of the body are deposited on the hands. The hands then come into contact with another object or surface through touching. Through this contact, the subject may leave their fingerprints behind. Fingerprints, as a medium for identification, date back to pottery in the middle ages as well as to finger and hand seals dating back to BC era.

Despite the advancement of other forensic disciplines, such as DNA, fingerprint evidence remains the workhorse of crime scene and criminalistics. Our fingers come into contact with the outside world more than any other area of our body. Whatever task we set out to employ, it invariably involves touching, grabbing, and moving objects. Thus, latent print work is very effective in crime scene investigation. Whatever the crime, the perpetrator likely touched, held, or moved an object or objects in the perpetration of their acts. This can include things like a knife or gun in a violent crime to a door, window, or safe in a burglary/theft. Even

a paper on which a note was written or a countertop in a bank or convenience store robbery. All of these areas are potential locations of fingerprint evidence.

Fingerprints found at crime scenes are generally separated into three categories. These are plastic, patent, and latent. Plastic prints are three dimensional and exist in pliable surfaces like wax, clay, or putty. These types of impressions are rare as the surface conditions need to be perfect for the formation of a plastic print. Patent prints are areas of friction ridge detail that are visible to the naked eye without any enhancement. These are created when the hand is soiled in a substance with a staining quality and then comes into contact with another surface. This includes situations like prints located in ink, blood, and grease. The last type prints are latent prints. Latent prints are defined as areas of friction ridge detail that are invisible to the naked eye and are only visible after some sort of processing is done to make the fingerprints visible. These are the most common in the field of forensic science to the extent that most crime labs' sections dealing with fingerprints are formally named the Latent Print Unit or Section.

Fingerprint Powders and Processing Variations

The most common way that latent prints are made visible is with the application of fingerprint powder. Fingerprint powder comes in innumerable forms and colors. For our purposes, we will concentrate on those with widespread use and acceptance. The most common colors are black, white, and silver/gray. Fingerprint powder originally only came in black as well as gray and was made with volcanic ash. Volcanic ash was of such a fine consistency that it worked well for latent print use and is still in use to this day in many labs and field units. Regular powder works best on smooth and nonporous surfaces. It is most often applied with fiberglass brushes. Although it should be noted that there is variation here based on the specific powder being used and individual's preferences and habits. The color of the fingerprint powder is chosen simply to create the greatest color contrast with the item being processed. So, if one was processing a dark colored surface, they would use a silver/gray powder. If one was processing a light-colored surface, they would use black powder. Providing the greatest contrast to the background makes it easier for the examiner to see the print and thereby increases the chances of the print being of value.

Another common type of powder is also available in magnetic form. The powder is made with a metallic quality that is attracted to a magnetic applicator. The brush is more of a magnetic wand used to hold and dispense the product. Experienced individuals processing areas for latent prints quickly find the specific uses and benefits of magnetic powder, which came about in the early 1960s. "Textured surfaces such as vinyl imitation-leather or lightly textured automobile dashboards or door panels often respond well to magnetic powder, where regular powder would pack into the low places in the texturing and make development of a good latent impossible" (Minutiae, the Lightning Powder Co 1997). Another distinct advantage of magnetic powder is that it is safer to use since "there is no brush with fibers to touch and possibly damage the print. The powder … is attracted by a magnet and carried as whiskers by a magnetic wand. Nothing but the powder itself touches the print" (Minutiae, the Lightning Powder Co 1997). Like traditional powder, magnetic powder comes in many varieties and colors.

The last category of fingerprint powder is fluorescent. This type of powder is available in both the traditional and magnetic forms. The difference with fluorescent powder is that it fluoresces under the correct wavelength of light. Fluorescent powder is highly beneficial when you are looking for prints on an item with a colorful or distracting background. As was stated earlier, they key is to provide a contrast for the examiner. If the background is simply too colorful or patterned to have a contrast, then fluorescent powder can be used. The drawback here is that an Alternate Light Source is needed to cause and view the fluorescence of the powder. This is similar to an ultraviolent (blacklight) light used to locate items that fluoresce.

Cyanoacrylate fuming is another important step in fingerprint processing methodology. Cyanoacrylate fuming is also commonly referred to as super glue fuming because cyanoacrylate is the main ingredient in superglue. This is most common with smaller moveable items that can be transported back to a crime laboratory for fuming in a designated fuming chamber. Items are placed in the chamber and then cyanoacrylate vapors are introduced to the chamber. These vapors are attracted to the amino acids that make up the friction ridge impression. The vapors adhere to these areas and polymerize. This makes the prints much more durable and less susceptible to accidental destruction. The greater stability also allows a criminalist to employ other processing techniques that would otherwise destroy a latent print, such as dye staining. Dye staining is another technique to visualize latent prints with the use of an alternate light source tuned to a specific wavelength.

There are other processes that will develop prints on a variety of surfaces. Chemicals like ninhydrin and iodine can be used on paper and porous surfaces like raw wood or cardboard. Cloth, fabric, and other flexible and overly porous items are generally not-conducive to latent print development. If areas of friction ridge detail are located on these surfaces, it is most commonly a patent print.

Areas of friction ridge detail can be collected and preserved through a variety of techniques. Prints in powder can simply be lifted with fingerprint tape or hinged lifters. This is not unlike thick packing tape where the adhesive side is placed over the developed print. The tape is then removed and the powdered print is then adhered to a background that contrasts in color to the powder used. There are also lifting techniques that work better for curved or textured surfaces such as lifters with a gelatin quality and silicone casting materials such as Mikrosil. One of the best and increasingly prevalent ways of collecting a latent print is through photography. This requires a trained Forensic Photographer as there are a number of photographic as well as legal considerations. However, this method is preferred as it captures the truest form of the friction ridge detail. Destruction of the print through a mishap or mistake in the lifting process is not a concern, and it is able to be digitally enhanced without a need to scan in the image. With nearly all plastic prints and some patent prints, photography is the only means to preserve the area. This is especially true if the print is on a large item that cannot simply be removed and brought to the lab, like a wall in a house. Prints that that require a specific light source, such as those developed with fluorescent powder or dye stain, can be photographed in their state of fluorescence, thereby eliminating the need for an examiner to fluoresce the print in order to view it.

Latent Print Examiners and Examinations

Once an area of friction ridge detail is located and collected, it is provided to a latent print examiner. This person will conduct a qualitative and quantitative analysis of the area of friction ridge detail. This is completed to determine if the print has enough detail and is of sufficient quality to conduct an examination. If the print is sufficient, it can be compared to other areas of ridge detail. It is standard practice to submit known print exemplars of victims and/or other individuals who may have left the print unrelated to the crime. This way, an examiner can determine if the print is that of a possible perpetrator or not. For example, in a burglary, if a crime scene team locates fingerprints on a safe where money was taken, they do not know if they recovered the prints of the perpetrator, or simply prints left by the homeowner/victim from the accessing the safe in their normal course of business. The latent print examiner needs the prints from all the people who had lawful access to the item to make sure it was not one of their prints that happened to be located and collected. By eliminating these individuals as the source of a fingerprint, it may be reliably presumed that the fingerprint was likely left by the person who perpetrated the crime, although that cannot be completely assumed and will need verified by the investigators.

Once this is completed the examiner can look at the prints and compare them to possible perpetrators of the crime in question. This can come in a variety of ways. Investigators may submit prints of possible suspects that were acquired in the course of their

investigation. Note that this would require suspects to willingly provide exemplars of their fingerprints, or a search warrant to have been granted that would allow the police to recover the known exemplars. Many state agencies have databases of known fingerprints and palm prints generally known as Automated Fingerprint Identification Systems or AFIS. In the United States of America, the FBI maintains a database of fingerprints and palm prints known as the Next Generation Identification System (NGI). This database includes submissions from all states and the municipalities located within them. A section of this database is the recorded fingerprints and palm prints taken when one is arrested and goes through the booking phase to verify and ensure that the identity is correct. As such, an investigator may ask an examiner to compare the fingerprints recovered from the scene to a suspect's fingerprints that are on file in an AFIS or NGI database from a previous arrest. If there are no suspects, then an investigator can request that the fingerprints are searched in AFIS or NGI against the entire database. Here the computer-assisted search can provide the examiner with a list of possible people who have similar prints. It does require an examiner to then evaluate the list of candidates provided by the computer and determine if there is in fact an identification. This is a common misconception by the public, who assumes from television and movies that the computer itself makes identifications. The computer only provides a list of potential matches and cannot make any final determinations.

When comparing a latent print to a known print, the examiner does a qualitative and quantitative analysis of the friction ridge impressions. Here an opinion is formed as to if there is sufficient uniqueness to eliminate all possible donors except this one. (Smooth skin contains hair, sebaceous glands and sweat glands while volar skin contains only sweat galnds.) Their opinion of identification is a subjective conclusion and may be expressed in different terms depending on their training, skill, agency procedures, and experience.

It should further be noted that the common practice in fingerprint laboratories, and a requirement in accredited labs, is that another examiner verifies the findings of the initial examiner. The practice most commonly followed is referred to as ACE-V. This stands for analysis, comparison, evaluation, and finally verification (Ashbaugh 1999).

The ACE-V process begins with simply the ACE portions which can contain multiple sessions of all three portions: analysis, comparison, and evaluation. Initially, the first print (the unknown or latent print) is analyzed. Next, the second print is analyzed, as needed. These are then compared to each other. "Eventually, the final analysis and comparison lead to the final evaluation. Many influences can affect the current ACE examination" (Vanderkolk 2011). This includes "knowledge and beliefs of uniqueness, persistency, and impression evidence in other types of forensic comparative sciences can influence the examination. Biases, pressures, or expectations can influence the examination. The examiner needs to be aware of other influences and conduct the examination so that these influences do not negatively affect the examination" (Vanderkolk 2011).

The verification is a form of peer review to verify the process and the objectivity (Ashbaugh 1999). This is a checkpoint necessary with the subjective nature of fingerprint comparisons. This can be done multiple ways and blind verifications where the initial examiner's findings are not revealed to the verifying person has become the method most recommended. This eliminates the chance of bias. It should be noted that these processes are very case specific, and it can be a fluid practice.

Forensic Biology/DNA

The forensic science discipline, which had made the most strides and gained the most attention in the recent past, is that of Forensic Biology, which is comprised of the disciplines of body fluid identification/serology and DNA analysis. This area can be of great value to investigators and provide information that is both relative and substantial in its investigative and evidentiary value. In this practice genetic material is used to answer questions pertaining to the investigation. Often during the course of our daily activity, we leave behind genetic material. This is as simple as remnants of saliva on coffee cups and water bottles, to

skin cells on the clothing we wear and items we hold. There are specific types of activity, of which the criminality may be in question that are more likely to produce and dispose of genetic material. This is most common with sex-related activity and death investigations.

Forensic Biology starts with and was preceded with a forensic discipline called Serology. This is the process of examination and analysis of different bodily fluids, blood included (James et al. 2014). Serologists verify that material collected at a crime scene is actually a body fluid such as saliva, semen, urine, or blood. In the case of blood, they may confirm that it is human, or some other species. It should be noted that often these are stains and can be degraded or deteriorated, making these process more difficult and separating serologists in forensics with the comparable practice in the medical field (James et al. 2014). Traditionally, this process was necessary before the material could be submitted to a DNA lab. In current day, some labs have a straight to DNA approach with items that do not need verification or clarification as to the substance submitted.

DNA broke into the world of forensic sciences in the 1980s and prior to this blood was only used to determine blood type (ABO) and thereby could eliminate or include individuals to the suspect pool. DNA is a long molecule in the cell in the form of a twisted ladder that is called a double helix. For the purposes of forensic identification, they focus on Short Tandem Repeats (STR). It should be noted that in the past this was done through RFLPs (Restriction Fragment Length Polymorphism), which an investigator may find in lab reports or evidence from older cases. The invention of Polymerase Chain Reaction (PCR) allows a scientist to amplify DNA. PCR is a technology that copies short segments of DNA millions of times in a process that resembles the way DNA is duplicated in the body (Fisher 2004). This is what has permitted scientists to have success with very small samples of bodily fluids recovered at a crime scene.

In a sexual encounter, there is likely to be a swapping and disbursement of body fluids. This includes saliva from kissing, licking, or holding items in one's mouth. In an investigation, this fluid can be recovered directly from the item kissed, licked, or held in the mouth as well as from surfaces that quickly thereafter came into contact with said item. For example, in a sexual assault, a woman is forcibly pulled into an alley. Then male perpetrator pulls down her shirt and bra and licks her bare breasts. He then exposes his penis from his pants and underwear and has her perform oral sex on him against her will. They are interrupted. He returns his penis to his pants and underwear and flees the area. She covers her breasts back up with her bra and shirt then seeks help. In investigating this crime, the perpetrator's DNA may be able to be recovered from the saliva he deposited onto the victim's bare breasts as well as the inside of her bra from when she returned her breasts to her bra – postassault. This can be especially beneficial of she bathes or otherwise cleans herself prior to a forensic examination. If the suspect is apprehended, the victim's saliva could possibly be recovered from his penis. Similarly, if this is not possible or able, there is a likelihood that some of her saliva may have been deposited on the inside of his underwear when he returned his penis to his underwear – postassault. Had they not been interrupted, and the suspect had ejaculated then there would also be the ability to collect his DNA from the cells in the ejaculate. If this is recovered at the scene, then it ties the suspect to the scene where it occurred. If it is on the victim's clothing or body, it helps to tie him to the victim due to the location of its recovery. It is extremely important for investigators to note from where samples were located and recovered. Had this hypothetical assault included any activity with the victim's vagina then the presence of vaginal fluid could also be possible. If the suspect would have penetrated her vagina with his fingers, or an object then it becomes possible to potentially locate traces of her vaginal fluid. This could be on the suspect's fingers or penis, or an object that may have been used to penetrate her vagina. If it is on the suspect's body and he has time to clean himself or there is a delay in time between the assault and his capture, it becomes increasingly likely that the fluids will have been washed off. However, with an object it may remain and that could help to tie him and the object to the assault.

Seminal and vaginal fluids are particularly probative to an investigation of a sexual nature because these fluids are only present due to sexual activity. Blood, saliva, and skin cells can be left behind through completely innocuous activity. This is not the case with seminal and vaginal fluid. There is a challenge for the investigator in that the presence of this fluid can confirm the activity occurred. If seminal fluid or spermatozoa are located on the orifice swabs collected in a sexual assault collection kit, then we know that penetration occurred (Fisher 2004). It does not prove that there was or was not consent, or specific motives and intent in behavior that may be criminal. Urine is also a substance from which genetic material can be processed evidentiarily, but with some difficulty.

While forensic biology plays a crucial role in crimes like sexual assaults, it is not limited to those types of crimes or investigations. Genetic material can be recovered from a number of situations. If someone is receiving threatening letters, they can be examined for saliva from licking the envelope. Burglary often requires force to enter the home or business. During this force, it is not uncommon for a perpetrator to injure themselves. This can be from shards of glass in a broken window to an injury sustained prying a lock open. This creates a situation where blood can be recovered from the scene. Moreover, this blood can tie them to the specific activity related to gaining entry if it is located there. If blood is found on the edge of broken glass, then in can be inferred that the suspect cut themselves on the broken glass as it could not have been deposited there prior to the glass being broken. The same holds true for any point of forced entry where damage occurs that did not previously exist.

Touch DNA has become a common topic in the evolution and advancement of DNA technologies. DNA testing originally required a larger sample that it currently does. The development of touch DNA has dramatically increased the number of items of evidence that can be used. In the 1980s, in order to perform DNA analysis forensic investigators needed a blood or semen stain about the size of a quarter (Houck and Houck 2008). With the advancement in the ability to amplify collected samples, labs have been able to process much smaller samples. This has allowed the testing on a small number of epithelial cells shed from the handler's skin. We are constantly shedding skin cells throughout our life and in our activities. Some of these activities allow for a more concentrated deposit, which can open the door for DNA testing. The best example of this is the clothing we wear. A shirt collar has constant and prolonged contact with your body. As such, it is an excellent potential source of touch DNA. The same principle applies to other clothing which has prolonged contact with your skin, to include hats and gloves. Hats and gloves are more commonly discarded and left behind, therefore becoming frequent objects collected during investigations. Items which are held for significant periods of time are likewise candidates for Touch DNA processing. For these though it is important that the item has a textured surface that is able to hold the skin cells and also that the person in question held it for a significant period of time or utilized it with a significant amount of force. A smooth item like a doorknob or a piece of silverware is unlikely to have an area capable of holding skin cells. Contrastingly, items like the checkered handle of a firearm or a rubber texturized grip of an aluminum baseball bat have a better chance of retaining shed skin cells. Even if the item has this textured surface, it is crucial that the person in question hold the item for a significant period of time. If one merely handles an item or only has it for a few minutes, it is unlikely that they would shed enough cells in that period of time to leave behind enough of a sample to yield any results. Other names for Touch DNA that can be more accurate are "Wearer DNA" or "Prolonged Contact DNA."

Once an item has been collected for potential DNA or a swab of a substance believed to be genetic material is submitted to a crime lab the first place it is analyzed is the Serology Section. That is unless, the lab's practices follow the direct to DNA approach mentioned above. Scientists in this section will screen the items or samples for the presence of biological materials. This is most commonly done visually, chemically, immunochemically, and microscopically. Alternate

Light Sources, which utilize specific wavelengths of visible light as discussed earlier in Latent Prints, are used here too, as many biological fluids fluoresce. Confirmatory tests can verify that the item is what it is presumed to be, such as blood, semen, and saliva. Urine can be screened for substances commonly found in urine. Some body fluids can also be verified as human and not from another species.

The most common form of DNA in forensics is nuclear DNA. These samples go through a four-step process of extraction, quantitation, amplification, and detection. The lab targets regions along the chromosome known as short tandem repeats (STR). This STR genetic profile can then be compared to other known genetic profiles. This can include profiles of the victim, suspect, or other involved parties. Through this comparison, a scientist can include or exclude individuals as contributors. If there are no known persons or samples with which it is to be compared, there is a database maintained by the government against which it can be searched, if the sample meets the criteria established by the FBI. This is known as CODIS, which is the Combined DNA Indexing System. Profiles can be uploaded to CODIS which will search the unknown profile against convicted offender and arrestee profiles, as well as unknown profiles from other open cases. If a hit occurs, then the laboratory will be able to provide either the name of an arrestee or convicted offender, or case information from a related case, as an investigative lead. So, if investigating a serial rapist, the investigators can determine other crimes that this person has likely perpetrated, or even other agencies that may be investigating the same unknown individual for like or other crimes.

Mitochondrial DNA is most commonly used where the DNA samples lack the quality or quantity for Nuclear DNA testing. mtDNA can come from items such as bone, hair, or environmentally damaged samples. mtDNA only follows the maternal lineage. mtDNA can be used in missing persons cases or with samples that are old and degraded where nuclear DNA in not present (Fisher 2004).

DNA processing can generally do several things to aid an investigation. It can link suspects and victims not only to each other, but also to the scene themselves of objects used in the commission of the act in contention. They can include or exclude individuals as suspects or victims. DNA processing can also help to establish the crime scene or where an act occurred as well as corroborate circumstances relevant to the case.

Conclusion

Despite the advancement of other disciplines in the forensic science arena, fingerprints continue to be the workhorse as the most used and widespread applicability through various criminal activities. While fingerprints is the most common forensic practice, DNA is the quickest advancing discipline and the one with the greatest future potential in scientific advances. There are already scientists getting more detailed results from samples and working on new techniques to gain useful information from smaller or degraded samples. The realm of DNA evidence is expected to continue to grow in its usefulness in criminal investigations.

Cross-References

- ▶ Investigations: Burglary
- ▶ Investigations: Polygraph Use
- ▶ Investigations: Sexual Assault

References

Ashbaugh, D. R. (1999). *Quantitative-qualitative friction ridge analysis: An introduction to basic and advanced ridgeology*. Boca Raton: CRC Press.

Fisher, B. A. (2004). *Techniques of crime scene investigation*. Boca Raton: CRC Press.

Houck, M., & Houck, L. (2008). What is touch DNA? *Scientific American, 299*, 108.

James, S. H., Nordby, J. J., & Bell, S. (2014). *Forensic science: An introduction to scientific and investigative techniques*. Boca Raton: CRC Press/Taylor & Francis Group.

Minutiae, the Lightning Powder Co. Newsletter, #43, July-August 1997.

Vanderkolk, J. R. (2011). *Examination process. Fingerprint sourcebook. Chapter 9*. Washington, DC: National Institute of Justice.

L

Law: Administrative

Kevin Govern
Ave Maria School of Law, Naples, USA

Keywords
Administrative Law · Rules · Procedures · Caselaw · Statutes · Administrative Procedures Act · Adjudication · Judicial Review

Definition

Administrative law is the branch of law governing the creation and operation of administrative agencies. It is also a body of rules, procedures, and principles created by government agencies and departments in order to carry out laws created by courts (*case law*) and legislatures (*statutes*).

Introduction

This entry summarizes federal and state/territorial administrative law as it affects security management and emergency management (McKinney 2018). Federal administrative law primarily concerns the powers and procedures of federal administering agencies in relation to the public (but usually not in criminal matters). It is the Congress that grants general and specific powers to various federal agencies through enabling legislation as well as the general laws for their fair and orderly administration. These executive powers are often quasi-legislative in nature (via rules and regulations applicable to a class of persons or organizations) or quasi-judicial in nature (via orders, adjudications, and decisions involving particular persons or organizations). The given powers are also subject to judicial review and interpretation. As industry and technology grew over the past 125 years, the Congress deemed it appropriate to delegate the details of administering laws to protect the public or enhance fairness to executive departments or independent regulatory agencies. Unlike the heads of executive departments and agencies, the heads of independent regulatory agencies generally do not serve at the pleasure of the president or have their rules and legislative recommendations reviewed first by OMB [Office of Management and Budget]. The first independent regulatory agency was the Interstate Commerce Commission established in 1887 (McKinney 2018).

Powers of Enabling Statute

An *enabling statute* may create an agency, authorize rulemaking, and empower agency rule enforcement. At the same time, other laws in the agency's expertise area may be enforced by the agency and then become agency standards and rules. Procedural rules are laws of agency methods and effect agency operations. Substantive laws which are enacted to protect rights

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

demand equal protection in administrative law as well as other areas of law (DOL 2018).

Federal Administrative Procedure Act (5 U.S.C. Subchapter II) (APA): The *APA*, officially enacted on June 11, 1946, is a US federal law that governs the way in which administrative agencies (positioned within the US federal government) may propose and subsequently establish regulations (APA 2018).

Model Administrative Procedure Act (Model State APA): The similar Model State APA was drafted by the National Conference of Commissioners on Uniform State Laws for oversight of state agencies. Not all states have adopted the model law wholesale. By comparison, the federal APA does not require systematic oversight of regulations prior to adoption as suggested by the Model APA (Oversight 2007).

Primary Types of Rules

The primary types of administrative rules are substantive rules that implement the intent of a law or statute, interpretive rules that provide explanation of law or action, and procedural rules that set forth procedures of an agency (Types of Rules 2018). The daily journal of the US government, the *Federal Register*, includes current issuances of documents from agencies, notices, presidential documents, proposed rules, and rules (Federal Register 2018). Regulations are first published in the *Federal Register* and then later appear in the Code of Federal Regulations (CFR). States, territories, and protectorates may have varying definitions relevant not just to administrative law generally but specifically regarding rules and their publication, and their availability in codes, manuals, and registers will also vary (Admin Rules 2018).

Agency Powers

What constitutes an agency is mandated by a legislature; e.g., § 551 of the APA defines each authority of the government of the United States but does not include the Congress, the courts of the United States, the governments of the territories or possessions of the United States, the government of the District of Columbia, and other exceptions (APA). An agency has diverse powers to set standards, make rules and regulations, take enforcement actions against those who refuse to obey the regulations, make decisions on those actions that come before it in claims and hearings, and investigate and take action regarding complaints on noncompliance with laws, agency rules, and regulations (APA).

Adjudication and Judicial Review

Administrative adjudication is the process by which an administrative agency issues an affirmative, negative, injunctive, or declaratory order. The formal proceedings before an administrative agency adopt the process of rule-making or adjudication (Administrative Adjudication 2018).

Judicial review is a process by which a court of law decides on the appropriateness of an agency's action in an appeal on the action. However, if there is a statutory prohibition on judicial review, the agency action is based on the agency's discretion. Some states create statutes that prohibit judicial review in administrative actions (Preclusion 2018).

The Administrative Procedure Act provides for comprehensive judicial review of agency actions. Any person adversely affected or aggrieved by agency action is entitled to judicial review as long as the action is a final agency action for which there is no other adequate remedy in a court (Yeboah 2001). The three criteria by which courts consider while deciding whether action of an agency is reviewable are as follows:

- The agency must have broad discretionary powers.
- Courts have to consider whether the action implicates any political, military, economic, or other choices not essentially legal in nature and, thus, whether the action is not readily susceptible to judicial review.
- Even actions committed to agency discretion by law are reviewable on grounds that the agency lacked jurisdiction, decision of the

agency resulted from impermissible influences, or such decision violates any constitutional, statutory, or regulatory command (Yeboah 2001).

In judicial review procedures, *Chevron* deference is a principle of administrative law requiring courts to defer to interpretations of statutes made by those government agencies charged with enforcing them, unless such interpretations are unreasonable. The principle is named for the 1984 Supreme Court case Chevron USA, Inc. vs. Natural Resources Defense Council, Inc. which involved a dispute over the Environmental Protection Agency's interpretation of a provision of the Clean Air Act Amendments of 1977 (Chevron 1984). Under *Chevron*, even if a court finds that another interpretation is reasonable, or even better than the agency's interpretation, it must defer to the agency's reasonable interpretation (Chevron 1984).

Conclusion

Administrative law is important to security and emergency management because both of those overlapping fields operate under laws that govern the creation and operation of administrative agencies. In order to understand how those agencies work, you must appreciate the creation, promulgation, enforcement, and appeal of rules, procedures, and principles created by government agencies and departments.

Cross-References

► Law: Specialized

References

5 U.S. Code. (2018). Chapter 5 – administrative procedure, Cornell Law School LII (APA), https://www.law.cornell.edu/uscode/text/5/part-I/chapter-5

Admin Rules. (2018). AdministrativeRules.org, http://www.administrativerules.org/administrative-rules/

Administrative Adjudication Law and Legal Definition. (2018). USLegal.com, https://definitions.uslegal.com/a/administrative-adjudication/

Chevron U.S.A., Inc. v. NRDC, 467 U.S. 837. (1984). cited with authority in David Kemp, Chevron deference: Your guide to understanding two of today's SCOTUS decisions, JUSTIA.com, 21 May 2012, https://lawblog.justia.com/2012/05/21/chevron-deference-your-guide-to-understanding-two-of-todays-scotus-decisions/

Federal Register. (2018). https://www.federalregister.gov/

McKinney, R. J. (2018). Federal administrative law: A brief overview, 3 May 2017 (McKinney), http://www.llsdc.org/assets/sourcebook/fed-admin-law.pdf.

Oversight and Insight: Legislative Review of Agencies and Lessons from the States, 121 Harv. L. Rev. 613. (2007). Oversight, http://www.harvardlawreview.org/issues/121/december07/Note_1047.php

See Preclusion of Judicial Review. (2018). USLegal.com, Preclusion, https://administrativelaw.uslegal.com/judicial-review-of-administrative-decisions/preclusion-of-judicial-review/

Types of Rules and Agency Statements. (2018). USLegal.com, https://administrativelaw.uslegal.com/administrative-agency-rulemaking/types-of-rules-and-agency-statements

United States Department of Labor, Office of workers/compensation programs. (2018). DOL, https://www.dol.gov/owcp/dfec/regs/compliance/feca550q.htm

Yeboah v. INS, 2001 U.S. Dist. LEXIS 17360 (E.D. Pa. Oct. 26, 2001). (2001). cited with authority in Judicial Review of Administrative Decisions, USLegal.com, https://administrativelaw.uslegal.com/judicial-review-of-administrative-decisions/

Further Reading

Administrative Conference of the United States website, https://www.acus.gov/

Administrative Law Guide, Library of Congress, https://www.loc.gov/law/help/administrative.php

Harvard Law School Office of Public Interest Advising. (2011) A guide to careers in administrative law, https://hls.harvard.edu/content/uploads/2011/08/adminlawguide.pdf

Law: Specialized

Kevin Govern
Ave Maria School of Law, Naples, USA

Keywords

Emergency Management Assistance Compact · EMAC · Federal Employees Compensation Act (FECA) · Federal Tort Claims Act · FTCA · Homeland Security

Presidential Directives (HSPD) · National Emergencies Act · NEA · National Response Framework · NRF · National Strategy Documents · Office of Biometric Identity Management · OBIM · Pandemic and All Hazards Preparedness Act (PAHPA) · Presidential Policy Directives · PPD · Public Health Service Act · Public Readiness and Emergency Preparedness Act · PREP Act · REAL ID · Robert T. Stafford Disaster Relief and Emergency Assistance Act · Stafford Act · Safety Act · Social Security Act · Volunteer Protection Act · Policies

Definition

Specialized law consisting of *compacts, statutes*, and *policies* governs the intersection of security management and emergency management.

Introduction

Specialized law affects everyone who works in the fields of security and emergency management. This entry summarizes some of the most significant prescriptions and proscriptions needed for routine day-to-day operations and emergency operations of security management and emergency management agencies which rely upon authorizations and appropriations to accomplish core missions. In the next section, some of the most important and commonly applied laws in those realms, laws that provide the basis for compacts between governments and private entities, as well as overarching policies for the way ahead, are described.

Laws (ASTHO 2018)

Routine day-to-day operations, emergency operations of security management as well as emergency management agencies rely upon authorizations and appropriations to accomplish core missions, e.g. preventing terrorism and enhancing security, securing and managing borders, enforcing and administering laws, safeguarding and securing cyberspace, and ensuring resilience to disasters, both natural and man-made (Homeland Security 2016). What follows is a selection of some of the most important and commonly applied laws in those realms and which laws also provide the basis for compacts between governments and private entities, as well as overarching policies for the way ahead.

The Emergency Management Assistance Compact (EMAC) is a congressionally authorized interstate mutual aid compact that provides a mechanism through which states can provide assistance to other states during emergencies. All states have joined EMAC by adopting model language into their state's statutes. EMAC addresses reimbursement, liability, compensation, and licensure issues (EMAC).

The Federal Employees Compensation Act (FECA) provides workers' compensation to civilian federal employees who are injured or killed during the course of their duties. Volunteers who may deploy in states under federal programs like the National Disaster Medical System or are otherwise deemed to be federal employees are covered under FECA (FECA).

The Federal Tort Claims Act (FTCA) permits lawsuits to be brought against federal government employees in certain circumstances. FTCA allows individuals to seek compensation when they are injured by federal employees acting within the scope of their duties. The act immunizes federal government employees from tort liability (except in certain instances); the federal government assumes an employee's role as defendant in a lawsuit against the employee. Volunteers of federal agencies deployed by those agencies are entitled to coverage under FTCA (FTCA).

The National Emergencies Act (NEA) allows the president to declare a national emergency, which triggers emergency authorities contained in other federal statutes. NEA does not contain any specific emergency authority on its own but relies on the emergency authorities in other statutes, such as the Public Health Service Act. President Obama used the NEA to declare the 2009 H1N1 influenza pandemic a national emergency.

A declaration under the NEA (or the Stafford Act) and a Section 318 public health emergency declaration are required before the HHS secretary can exercise Social Security Act Section 1135 waiver authority (NEA).

The OBIM or *Office of Biometric Identity Management* (*OBIM*), formerly US-VISIT, provides biometric identity services to DHS and its mission partners that advance informed decision-making by producing accurate, timely, and high-fidelity biometric identity information while protecting individuals' privacy and civil liberties (OBIM).

The Pandemic and All-Hazards Preparedness Act (PAHPA) addresses the organization of public health emergency preparedness and response activities and authorizes programs concerning medical surge capacity, the capacity of states and localities to prepare for and respond to public health emergencies, and the development of countermeasures to biological threats (the Biodefense Advanced Research and Development Authority [BARDA]). Many of the offices and programs within the Department of Health and Human Services (HHS) that state public health preparedness programs interact with on a daily basis were developed or refined through PAHPA, including the Office of the Assistant Secretary for Preparedness and Response, grant programs such as Public Health Emergency Preparedness (PHEP) grants, the Hospital Preparedness Program, and the Healthcare Facility Partnership Program. The act also focuses on the needs of at-risk populations in emergency planning and response. PAHPA was reauthorized in March 2013 in the Pandemic and All-Hazards Preparedness Reauthorization Act (PAHPA).

The Public Health Service Act Section 319 authorizes the HHS secretary to determine that a public health emergency exists, which triggers emergency powers that permit the federal government to assist state and local governments, suspend or modify certain legal requirements, and expend available funds to address public health emergencies. A Section 319 public health emergency declaration is separate and distinct from a presidential declaration under the National Emergencies Act or the Stafford Act. The secretary does not need a presidential declaration to issue a public health emergency declaration under Section 319; however, a presidential declaration is required in addition to a Section 319 declaration if the secretary wants to exercise waiver authority under Social Security Act Section 1135. Other sections of the Public Health Service Act, including Sections 301 and 311, permit the secretary to render assistance to states and localities without declaring a public health emergency (PHSA).

The Public Readiness and Emergency Preparedness Act (PREP Act) authorizes the HHS secretary to issue a declaration that provides immunity from tort liability for claims of loss caused by countermeasures against diseases or other threats of public health emergencies. The act covers persons and entities involved in the manufacture, testing, distribution, administration, and use of covered countermeasures. A PREP Act declaration is different from and independent of other federal emergency declarations. A separate emergency declaration under Public Health Service Act Section 319 or another statute is not required for PREP Act immunities take effect (PREP Act).

The REAL ID Act, passed by Congress in 2005, enacted the 9/11 Commission's recommendation that the federal government "set standards for the issuance of sources of identification, such as driver's licenses." The purposes covered by the Act are accessing federal facilities, entering nuclear power plants, and boarding federally regulated commercial aircraft (REAL ID).

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) authorizes the delivery of federal emergency technical, financial, logistical, and other assistance to states and localities. A governor must first determine that an event overwhelms the state's capacity to respond and request a presidential declaration under the Stafford Act before the president can declare all or a portion of a state a "major disaster" or "emergency" area. The Federal Emergency Management Agency (FEMA) coordinates administration of disaster relief resources and assistance to states. The President can declare an emergency without first receiving a gubernatorial

request if the emergency involves an area of federal primary responsibility such as a federal building. A Stafford Act declaration can be used to trigger other public health emergency response authorities such as Social Security Act Section 1135 waiver authorities (Stafford Act).

The SAFETY Act, as part of the Homeland Security Act of 2002, Public Law 107-296, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act (*SAFETY Act*) of 2002. The *SAFETY Act* provides incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management (SAFETY Act).

The Social Security Act Section 1135 authorizes the HHS secretary to temporarily waive or modify certain Medicare, Medicaid, Children's Health Insurance Program (CHIP), and Health Insurance Portability and Accountability Act (HIPAA) requirements affecting healthcare facilities and providers during national emergencies. Section 1135 waivers require both a presidential declaration under the National Emergencies Act or Stafford Act and a public health emergency determination by the HHS secretary under Public Health Service Act Section 319. Once the 1135 waiver authority has been issued, individual providers' requirements are not automatically modified; the waivers are implemented on a case-by-case basis through the Centers for Medicare and Medicaid Services, HHS regional offices, and state health facility survey agencies (SSA).

The Volunteer Protection Act of 1997 provides immunity from ordinary negligence to volunteers of nonprofit organizations or governmental entities. It does not cover gross negligence, willful misconduct, recklessness, or acts committed by the volunteer while intoxicated or operating a motor vehicle. It does not cover organizational entities of any type or persons volunteering at private businesses. The act does not require a declared emergency for its protections to apply (VPA).

Policies

Homeland Security Presidential Directives (HSPDs) and Presidential Policy Directives (PPDs) announce executive policies regarding, among other things, homeland security issues. HSPDs and PPDs establish policies, strategies, and frameworks directing executive agency activities on a range of homeland security matters. Directives important for public health are HSPD-5 (management of domestic incidents), PPD-8 (national preparedness – formerly HSPD-8), and HSPD-21 (public health and medical preparedness) (HSPD).

The National Incident Management System (NIMS) is a system of incident command developed by the Department of Homeland Security to coordinate emergency response efforts at all levels of government and the private sector. It is a scalable system that can be used for events and incidents of all sizes regardless of whether a federal emergency or disaster is declared under the Stafford Act (NIMS).

The National Response Framework (NRF) is a Department of Homeland Security policy document that uses a national, all-hazards approach to describe and integrate roles for governments at all levels and the private sector in preparing, responding, and recovering from emergencies of all sizes, regardless of whether an emergency is declared. The NRF uses NIMS to coordinate response activities. The NRF includes 15 Emergency Support Function (ESF) supplemental documents that detail the roles and responsibilities of governmental and certain private sector capacities in key areas. Relevant to public health are ESF-8 (public health and medical services) and ESF-6 (mass care, emergency assistance, housing, and human services) (NRF).

National Strategy Documents arise from federal legislation and directives that mandate the creation of various strategies and plans to chart national emergency planning and response activities. These national strategy documents are intended to complement the National Response Framework and address plans for coordinating with state, local, territorial, and tribal governments and the private sector. Relevant national strategy documents for public health include the National Health Security Strategy, the National Strategy for Pandemic Influenza, and the National Strategy for Homeland Security (NSD).

Conclusion

The enumerated specialized laws, consisting of *compacts*, *statutes*, and *policies* govern the intersection of security management and emergency management, affecting not only the governance of government agencies and departments but how they render security management and emergency management services.

Cross-References

► Law: Administrative

References

Emergency Authority and Immunity Toolkit, Association of State and Territorial Health Officials. (2018). NEA, Available at http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Authority-and-Immunity-Toolkit/National-Emergencies-Act,-Sections-201-and-301-Fact-Sheet/

Emergency Authority and Immunity Toolkit, Public Health Service Act, Section 319, Association of State and Territorial Health Officials. (2018). PHSA, http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Authority-and-Immunity-Toolkit/Public-Health-Service-Act,-Section-319-Fact-Sheet/

Emergency Management Assistance Compact (EMAC). (2018). https://www.emacweb.org/

Emergency Volunteer Toolkit, Volunteer Protection Acts and Good Samaritan Laws, Association of State and Territorial Health Officials. (2018). VPA, Available at http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Volunteer-Toolkit/Volunteer-Protection-Acts-and-Good-Samaritan-Laws-Fact-Sheet/

Executive Overview, Key Federal Laws and Policies Regarding Emergency Authority and Immunity, Association of State and Territorial Health Officials (ASTHO). (2018). Available at http://www.astho.org/Programs/Preparedness/Public-Health-Emergency-Law/Emergency-Authority-and-Immunity-Toolkit/Key-Federal-Laws-and-Policies-Regarding-Emergency-Authority-and-Immunity/

Federal Emergency Management Agency, National response framework. (2016, June 16). 3rd edn, NRF, https://www.fema.gov/media-library/assets/documents/117791

Federal Emergency Management Agency, Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93–288) as amended. (2018). Stafford Act, https://www.fema.gov/robert-t-stafford-disaster-relief-and-emergency-assistance-act-public-law-93-288-amended

Health Resources and Services Administration – HRSA Health Center Program. (2018). FTCA, https://www.dol.gov/owcp/dfec/regs/compliance/feca550q.htm

Homeland Security. (2016). Our Mission, last published 11 May 2016, https://www.dhs.gov/our-mission

Homeland Security Digital Library, National strategy documents. (2018, Feb 13). NSD, https://www.hsdl.org/c/national-strategy-documents/

Homeland Security, NIMS: Frequently asked questions. (2018). NIMS, https://www.fema.gov/pdf/emergency/nims/nimsfaqs.pdf

Homeland Security, Office of biometric identity management. (2018). OBIM, https://www.dhs.gov/obim

Homeland Security, Presidential Directives. (2018, Feb 8). HSPD, https://www.dhs.gov/presidential-directives

Homeland Security, REAL ID. (2018). REAL ID, https://www.dhs.gov/real-id

Homeland Security, The Office of SAFETY Act Implementation. (2018). (SAFETY Act), https://www.dhs.gov/science-and-technology/safety-act

Social Security Administration. (2018). Compilation of the social security laws, Authority to waive requirements during national emergencies, Sec. e1135 [42 U.S.C. 1320b-5], SSA, https://www.ssa.gov/OP_Home/ssact/title11/1135.htm

U.S. Department of Health and Human Services, Public Health Emergency – Pandemic and All Hazards Preparedness Act. (2018). PAHPA, https://www.phe.gov/preparedness/legal/pahpa/pages/default.aspx

U.S. Department of Health and Human Services, Public Health Emergency – Public Readiness and Emergency Preparedness Act. (2018). PREP Act, https://www.phe.gov/Preparedness/legal/prepact/Pages/default.aspx

United States Department of Labor, Officee of Workers' Compensation Programs. (2018). FECA, https://www.dol.gov/owcp/dfec/regs/compliance/feca550q.htm

Further Reading

Defense Support of Civil Authorities. (2013, July 31) Joint publication 3–28, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf

Govern, K. H. (2016). Defense support of civil authorities: An examination of trends impacting upon police militarization. *Washington and Lee Journal of Civil Rights and Social Justice, 23*(1), 89–134. Fall 2016. Available at SSRN: https://ssrn.com/abstract=2978460.

Homeland Defense Integration & Defense Support to Civil Authorities (DSCA), http://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-Global-Security/Homeland-Defense-Integration-DSCA/

M

Machine Learning

Douglas E. Salane
Mathematics and Computer Science Department, John Jay College of Criminal Justice, New York, NY, USA

Keywords
Machine learning · Privacy · Security · Automated systems · Social media

Definition

Machine learning (ML) describes a wide array of algorithms that analyze data and enable a computer to make predictions.

Introduction

Machine learning (ML) describes a wide array of algorithms that analyze data and enable a computer to make predictions. Differing from traditional statistical analysis, which makes various assumptions about data, algorithms identified as machine learning typically let the data do the talking. ML at this point is coming to mean just about any automated system that learns from data, or which was created by learning from a data set, a so-called training set, and then used to make predications based on data not seen previously. Unlike a static program that takes data in and outputs an answer, a program using ML techniques takes data as input and based on the data can modify itself to be more effective at making predications and achieving its objective. Increasingly, ML techniques are used in some part of the automated systems with which users interact, for example, a natural language interface relies on ML techniques. Already many devices utilize ML algorithms and operate independently, self-driving vehicles being one such example.

Users are exposed to ML algorithms every day, for example, when they access any web site that makes recommendations or when they receive targeted ads. Indeed, many of the algorithms today classified as ML algorithms including search engines have been around for quite some time. More recent applications include facial recognition, medical diagnosis, fraud detection, and spam detection. ML plays a key role in robotics, for example, allowing computers to identify objects. Classification, based on test data (supervised learning) or without prior data (unsupervised learning), is an important subfield of ML. Such algorithms often play a prominent role in determining who is a credit risk, who gets paroled or who gets the job.

Several advances in computing have allowed the ML community to flourish in recent years. Certainly, increased computational power and storage, especially in small devices, has played a key role. The ability to design an algorithm that learns from data but keeps the code largely fixed

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

in size has been very important as well. Expert systems had been around for years. However, these systems, which tried to incorporate expert knowledge, required code sizes to grow and become increasingly complex and unwieldly.

Many experts in the field point out ML techniques are often heuristic. In many problem areas, designers know how methods work on test data but cannot guarantee they will always perform as expected on data not seen previously. Despite impressive successes, many in the field still describe ML as part science and part alchemy.

There are two key reasons for the widespread rise in interest in ML. First, it has enabled the development of smart devices that can respond to a variety of situations, even situations that have never occurred before. Second, in almost any field, too much data is being created too rapidly for humans to process them without some type of intelligent digital assistance. In the medical field, without such assistance, it is impossible for medical researchers to be aware of all the publications, clinical trials, and drug interactions that might impact their work.

As ML-based systems proliferate and reliance upon them increases, these systems will present significant privacy and security challenges. The remainder of this entry describes some of the privacy and security concerns surrounding ML-based systems. In many instances, ML-based systems will also provide the solutions.

Privacy Concerns

Although privacy in the Internet age has long been an issue, no one has determined how to reconcile privacy risks with the current business models that make Internet services available. Simply providing more user control of privacy settings is not working. A recent review of the privacy literature concludes "users are often unaware of the information they are sharing, unaware of how it can be used, and even in rare situations when they have full knowledge of the consequences of sharing, uncertain of their own preferences" (Acquisti et al. 2015, p. 513). The research examined also shows user privacy decisions are impacted by context, for example, users are more likely to release sensitive information to well-known sites such as Facebook rather than lesser known sites. In addition, users are easily influenced in privacy attitudes by small rewards that can change privacy concerns. Users are quick to release data to gain a clear short-term benefit such as the use of an Internet-based service but prone to ignore the longer-term not so clearly defined risks of providing data or even just using the service.

On the other hand, when it comes to data collection, social media sites such as Facebook have a clearly defined purpose – collect as much data as possible and make every effort to monetize it. ML provides numerous opportunities to combine data from many sources to provide detailed profiles of people which are made available for sale. Not only data but full psychological profiles are now possible. Even detection and analysis of emotions are being considered with ML techniques (Gayo-Avello 2018). Increasingly, users cannot know the consequences of releasing data.

In his highly popular book, *The Master Algorithm*, Pedro Domingos describes a model for the future where the way users interact with the digital world is through a "digital half," essentially an ML-based program that presents users to the digital world and presents the digital world to them (Domingos 2015, p. 269). In many ways, this already is occurring, although not to the level anticipated in the book. The key question is who will control this technology and how will it be used. Right now, the motivation for providing such a service is advertising revenue. This front end, which people will rely on to access the digital world, will make decisions for them and know them intimately. It would likely incorporate current research that will allow the ML algorithm to gauge the mood of humans when using the system. One of the concerns is that users may not even be able to participate effectively in twenty-first century economic and social activities without such a front end or digital half.

Security Concerns

Although often portrayed as conflicting goals, without privacy there is no security. A fundamental tenet of security is the "need to know." It is usually

applied to classified information but is widely used by organizations and individuals to limit the damage done from the release of information, particularly by insiders. Aleksandr Kogan is a Cambridge University researcher hired by Cambridge Analytical to harvest data from tens of millions of Facebook profiles, data which was later used in the 2016 election without user consent. In an interview on April 23, 2018, Kogan, who had a long-standing relationship with Facebook, commented that the Facebook app can transfer and sell user data for up to year and half without notification from Facebook. He went on to say that social media platforms cannot be relied upon to police their sites, even if developers violate their policies. The basic business models of Internet companies create extreme incentives to share data with developers and advertisers, not to limit who has access to data nor to police privacy policies. Certainly, current business models, where users give away rights to data and how it is used, would be intolerable in a world where a digital half is needed to access the digital world and interact with it on a user's behalf.

As would be expected, hackers are also taking advantage of ML. An important Internet security challenge is the social botnet (Ford 2016). Social bots are computers running algorithms that automatically produce content and are able to interact with humans or computers and imitate human behavior, the classic idea of what artificial intelligence means. Such algorithms frequently use a range of machine learning techniques to interpret natural language, respond to queries, and infiltrate other systems. By commandeering a large collection of social bots, attackers can have a significant presence in social media which they then can use for a variety of possibly malicious or at least disingenuous purposes (Ferrara et al. 2016). Such bots may be used to artificially inflate support for a political candidate or to denigrate a candidate. Misinformation gains credibility by the mere fact that the collection of social bots appears to be individuals expressing an opinion or shared belief. Such bots have also played a role in click fraud and classic pump and dump schemes to inflate the value of stocks. ML algorithms make it much harder to determine whether users are bots or humans.

On the other hand, ML techniques are a key technology used to detect social bots. A bot that can change its behavior to adapt to its environment is hard to detect with standard algorithms. ML algorithms focus on general behavioral patterns to detect these bots. Rather than have an expert system try to predict all types of behavior, these programs are able to learn the behavior of a wide range of bots and then determine what computer is a bot and which one is a legitimate user (Davis et al. 2016). Stanford University now offers a course in ML-based bot detection. On the other hand, at Black Hat conferences, speakers discuss techniques on how to avoid ML-based bot detection. The age where security depends on an ML arms race may have arrived.

Increasingly, Americans are getting news from social media sites. A recent Pew Research Center report indicates that about 67% of US adults get some news from social media sites, up from about 62% in 2016 (Pew Research Center 2017). The report also states that Facebook is by far the largest social media news source with over 45% of US adults getting news from this site.

Social media sites rely heavily on machine learning algorithms to determine user preferences and interests. The sites provide news feeds and other news items that reflect those preferences. Many people claim this results in an increasing level of polarization and isolation of users as they predominantly receive news items that fit their profile and current notions (Lynch 2016). Those trying to influence political and social onions have a receptive audience for stories that support or harden a political position or social view. Some authors refer to this as a "filter bubble," since users are shielded from information that they do not like even if it is relevant to the discussion (Kelly 2016, p. 170).

Despite widespread belief in the value of disintermediation (i.e., no editors and anyone can post anything), social media sites now find themselves in the unenviable position of having to monitor content to filter out, among other things, violent extremist views, hate speech, pornographic material, and fake news. Again, machine learning algorithms are the way to examine the massive amount of content that is posted daily on social media sites. Blocking and filtering, however, reflect the biases of those who chose the data to train the ML algorithms used.

According to a New York Times report, YouTube removed over 8 million videos in the first quarter of 2018, 80% of which were removed with no human intervention (Wakabayashi 2018). Using ML techniques, social media sites, which for most Internet users provide a window to the information on the Web, are becoming content sensors for a large portion of the world's population.

Conclusion

In the foreseeable future, human lives will be dominated by automated systems which use a variety of ML algorithms. Users will most likely need some type of digital half to access and interact with the digital world. Users, however, cannot know the risks to privacy and security with the current state of digital world. What happens in an ML-driven world where users interact with algorithms that can practically imitate human behavior? ML offers incredible capabilities to take advantage of data, improve services, and gain knowledge. For Internet users, the benefits and risks will depend largely upon who controls these ML-based systems and how they are used.

Cross-References

- ▶ Cybersecurity: Practice
- ▶ Data Protection

References

Acquisti, A., Brandiamarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Davis, C., Ferrara, E., Flammini, A., Menczer, F., & Varol, O. (2016). BotOrNot: A system to evaluate social bots. In *WWW'16 companion* (pp. 273–274). Montreal: ACM.

Domingos, P. (2015). *The master algorithm*. New York: Basic Books.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM, 59*(7), 96–104.

Ford, M. (2016). *Rise of the robots*. New York: Basic Books.

Gayo-Avello, D. (2018, April 1). Social media won't free us. *Computing Edge*, pp. 42–51.

Kelly, K. (2016). *The inevitable: Understanding the 12 technological forces that will shape our future*. New York: Penguin Books.

Lynch, M. P. (2016). *The internet of US: Knowing more and understanding less in the age of big data*. New York: Liveright Publishing Corporation.

Pew Research Center. (2017). *News use across social media platforms.* Retrieved 10 March 2018, from http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/

Wakabayashi, D. (2018, Apr 24). You Tube says computers are catching video pitfals. *The New York Times*, p. B3.

Further Reading

Hof, R. D. (2018). Deep Learning: With massive amounts of computational power, machines can now recognize objects in real time. *MIT Technology Review*. Available at https://www.technologyreview.com/s/513696/deep-learning/. Retrieved 5 April 2018.

Kleinberg, J., Ludwig, J., Mullainathan, S. (2016, December 8). A guide to solving practical problems with machine learning. *Harvard Business Review.* Available at https://hbr.org/2016/12/a-guide-to-solving-social-problems-with-machine-learning. Retrieved 1 March 2018

Maritime Security: Acceptable Risks

Michael A. Edgerton
HudsonTrident., Inc, Camden, NJ, USA

Keywords

Maritime security · Risk · Threat · Vulnerability · Impact · Risk tolerance · Business impact assessment · Recovery time objective · Recovery point objective · Shipping · Port security · Maritime domain · Supply chain · Risk register · Risk treatment · Risk acceptance · Risk avoidance · Risk transfer · Risk reduction

Definition

Acceptable risks in maritime security are those that are determined to be residual risk after risk treatments have been implemented or have been

accepted after a rigorous and defensible security risk assessment has been conducted. Acceptable risks fall within the risk owner's risk tolerance.

Introduction

The maritime domain is a diverse and complex, multinational environment that does not easily lend itself to universally acceptable risks. Therefore, the key to understanding risk management and the determination of acceptable risks in the maritime domain is to understand the unique features of the maritime domain as well as key considerations in determining acceptable risks in maritime security. This entry provides an overview of the maritime domain and its unique characteristics, introduces the concept of security risk and its components, and identifies the concepts of risk tolerance and treatment as key elements in the determination and management of acceptable risks. Finally, the entry summarizes the challenges and unique considerations required to determine acceptable security risk within the maritime operating environment.

The Maritime Domain

In order to determine acceptable maritime security risks, the unique characteristics of the global maritime domain must be highlighted to provide an adequate context for the determination of acceptable risk. The maritime domain is fully reflective of the increased globalization of international trade as it transcends conventional understandings of legal jurisdictions and territory (Sakhuja 2010).

The maritime domain is characterized by six important factors. First, vessels and ports are increasingly multinational in nature. For example, it is not uncommon for a ship to be flagged in one country, owned or managed in another country, and crewed by persons from several other countries with no citizen of the flag state actually on the vessel. Additionally, ports may be operated by multinational operators in exchange for concessions that allow for a high degree of autonomous operations (Edgerton 2013).

Second, the global maritime environment is international as well as multinational in nature. By virtue of the nature of international trade, which is overwhelmingly transported by sea, the maritime operating environment is international. Vessels travel across international boundaries, as well as between continents in conducting their business. This has the effect of making the security conditions on ships, as well in all ports in a ship's voyage, a potential risk consideration for other countries. For example, if a ship transits from Indonesia to a US port via South Africa, the security conditions in both the Indonesian and South African ports are of interest to US authorities.

Third, as most of the world's oceans do not belong to any state, these are considered to be ungoverned spaces. These large swaths of the Earth's surface are under no country's jurisdiction which can serve to complicate security and enforcement activity. With the exception of Antarctica, and the aviation sector, this unique situation can make risk assessment challenging as legal authorities and jurisdictions are often unclear.

Fourth, maritime security is not easily pigeonholed into one isolated category, instead it is considered intersectoral. The maritime domain intersects with the broader transportation sector, especially where there are vital intermodal connections with roads and railways at seaports. Further, there is a strong interconnection with the energy sector as many oil and gas faculties are also ports where tankers load and unload cargo in addition to the large presence of off-shore oil and gas production facilities (United States Government 2007).

Fifth, and perhaps most importantly, the maritime operating environment is inexorably connected to, and part of, the global supply chain (World Bank 2009). Since most of the goods transported around the world are borne by ships and loaded and unloaded at seaports, any long-term or large-scale disruption of international shipping would have an extremely deleterious effect on world trade.

Sixth, the maritime industry is data-intensive, with millions of shipments and associated financial transactions underway at any given day,

coupled with the increase in reliance on digital systems to transfer and store information. In particular, the data includes contracts, banking information, personal information for employees and access control, container contents and security seal numbers, and other key information across the globe. Consequently, the data within the maritime industry is of potentially high value to those persons with nefarious intent, such as criminals and terrorists (Ahokas and Kiiski 2017).

Components of Risk

In determining acceptable risk in maritime security, the components to be assessed must be identified. While there are several accepted standards that provide guidance in the assessment of risk and provide definitions of the component, a basic and sound approach to *security* risk is use of the following formula (Fig. 1). The idea is that risk is perceived as the combination of threat, vulnerability, and impact.

As shown in Fig. 1, threat is the understanding of *who* potentially intends to carry out a harmful act. Vulnerability is the determination of *how easy or hard* it is to carry out a harmful act. Impact is an assessment of *what the results* of the harmful impact would be and how severe the results would be.

There are also a number for definitions of risk, but for the purposes of security, risk is the potential for unwanted or harmful events to occur (Bichou 2008). These definitions and components are specific to security and different from other risk approaches where risk may be considered a neutral state. For security professionals, risk is inherently negative.

Maritime Security: Acceptable Risks, Fig. 1 "Risk components"

Assessing Risk

Assessing risk involves putting a relative value to the risks identified and prioritizing those risks in a risk register. This process requires the participation of a fairly wide variety of stakeholders to include, at a minimum, security officials, industry experts, facility and vessel owners, and operators. Before the overall risk is assessed and determined, the individual components of risk must be assessed against the identified scenarios.

The following are general approaches to assessing each risk component – threats, vulnerability, and impact (Edgerton 2013). Threats are assessed by determining the intent, capability, history, and targeting of the actor or group. Threats must also be assessed in the context of the security environment. If the security environment is robust and effective, the threat may be lessened. Conversely, if the security environment is permissive and corrupt or ineffective, the threat may be greater.

Vulnerability can be assessed through a thorough review of the security measures in place. Further, vulnerability assessments may be aided by the execution of adversary pathway assessments whereby the potential routes and methods of the adversary combined with a knowledge of the potential methods and objectives that may be employed by the threat actors are used to determine the weaknesses in existing security measures.

Finally, assessing impact requires a nuanced understanding of not only the physical and near-term consequences of an adverse event but an assessment of the potential greater impacts including regional, national, and international security, economic impacts, and health and safety impacts. This assessment requires the participation of experts from many disciplines outside of the security profession.

The assessment of each component can be quantified against established standards of measure as desired in order to provide the ability to prioritize them.

Risk Tolerance

In order to determine the acceptable risks to maritime security, the risk tolerance of the

organization which has been assessed must be determined before proper treatment actions can be implemented (Institute of Risk Management n.d.). Every organization, whether it is a governmental organization or a private sector owner or operator of an element of the maritime environment, has its own level of risk tolerance. Some organizations are willing to tolerate higher risks in order to maximize efficiency or revenue while others are fundamentally risk averse. For example, seaport management teams may have widely divergent levels of risk tolerance. One seaport may consider a certain level of cargo theft and pilferage to be an acceptable "cost of doing business," while another may be much less tolerant of such activity.

In many cases, organizations have not undergone an attempt to formally determine or document their risk tolerance at the enterprise level (Risk and Insurance Management Society 2017). Possible reasons include:

- The organization determines risk tolerance in an ad hoc manner through deliberations with senior and middle management.
- The formal process of determining risk tolerance can be extremely uncomfortable as most people would prefer to not have to determine how much disruption or damage, their organization can withstand.
- There is often a reluctance to document risk tolerance as it then becomes potentially discoverable in litigation.

However, in order to determine acceptable risk levels, a formal risk tolerance exercise should be undertaken.

A key component that can inform the level of risk that an organization is willing to accept, can include a Business Impact Analysis (BIA) study and any associated business continuity and recovery planning. The findings of a BIA and recovery and continuity plans, however, often include information that is important to the determination of acceptable risk (*ISO/TS 22317:*2015*; Societal Security* 2015*)*. This key information includes two types of objectives. First, recovery time objectives refers to how fast key functions must be restored before unacceptable impacts are realized. Recovery point objectives, in contrast, refer to what level key functions must be restored in order to maintain an acceptable level of operations. Additional factors to be considered in determining risk tolerance include the level and adequacy of insurance that the organization has, the ability to shift operations to other locations or vendors, and the culture of the organization.

Treating Risk

Risk treatment is the process of determining how security risks should be addressed based on the risk tolerances identified and the assessed severity of the risk. Risk treatment is the activities to be undertaken to manage risk once that risk has been identified and assessed (*ISO 31000:*2018*; Risk management – Guidelines* 2018).

Once maritime risk has been assessed and prioritized and the level acceptable risk unique to a specific organization or company has been determined, risk treatment options are considered in order to bring risk to acceptable levels. While *risk mitigation* is often used in terms of addressing risk, there are actually four risk treatment options, which can be implemented separately or combined as appropriate.

The selection of the appropriate treatment option is directly relevant to the level of acceptable risk that has been determined. Risk acceptance is at the first level in which the risk does not require any treatment and can remain as assessed. The risk falls within the parameter of risk tolerance that has been determined. Risk avoidance is at the second level in which the risk is either sufficiently serious with no effective way to reduce it or would only provide such a minimal benefit to the organization that the seriousness of the risk outweighs any benefits. In this case, the risk may be avoided. Risk transfer is at the third level such that the risk has been assessed, but the most effective way to address the risk is to transfer the risk to another entity. Insurance is often cited as the most common instrument for transferring risk. Risk reduction is at the fourth level and means that the risk is reduced (in some cases,

eliminated) to a level that is acceptable to management. Once the risk has been reduced to a level assessed to be *As Low as Reasonably Acceptable (ALARP),* additional risk treatment can be applied. In some cases, the remaining, or residual risk, can be transferred. Otherwise, it is accepted.

Risk in the Context of Maritime Security

Maritime security encompasses a number of interrelated concerns, threats, and disciplines (Bichou 2008). These include:

- Maritime terrorism targeting ships and ports.
- Supply chain security in which cargo being transported by sea is susceptible to exploitation by criminal or terrorist groups.
- Smuggling of persons and contraband by vessels or via cargo.
- Cargo theft and pilferage.
- High-jacking and kidnapping.
- Piracy and armed robbery at sea.

Each of these threats require potentially different solutions that range from international governance structures such as treaties and codes, to enhanced maritime domain awareness through technology, naval, and coast guard forces, and command and control, to the development of commercial programs to incentivize good security management in the private sector.

Identifying Acceptable Risks in Maritime Security

There is no globally accepted list of acceptable risks in maritime security because the issue of maritime security is so complex and global in nature that there cannot be one approach to assessing and managing the acceptable risks to maritime security. Determining acceptable risks and the appropriate treatments is the function of a deliberate and defensible process of risk identification, assessment, and treatment based on the risk tolerance of the organization carrying out the assessment, whether it is a government or a private sector business. Further, the level of acceptable risks varies among public organizations and commercial entities, whose goals and objectives may not be aligned. Additionally, organizational culture and the maturity of management in assessing and addressing risk are contributing factors in the determination of acceptable risk in maritime security.

Conclusion

Identifying and managing acceptable risks in the maritime industry is a multidisciplinary activity that requires input from experts in maritime affairs, security, law, supply chain, economics, trade, and insurance. Determining acceptable risks will vary among organizations based on their culture as well as the results of other factors such as their ability to recover quickly or divert operations to other ports, ships, or locations. For governments, the determination of acceptable risks may also be driven by national and international politics and perceptions.

In maritime security, the primary considerations for the determination of acceptable risk hinge on the results of the assessment process informed by a broad spectrum of stakeholders. Due to the complexity of the maritime domain, it is impossible to clearly define specific criteria that are universally accepted in determining an acceptable level of risk. Therefore, the most advantageous approach to determining acceptable risk is through a well-defined and defensible process of risk assessment and treatment.

Cross-References

- ▶ Border Security
- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Cybersecurity: Practice

- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
- ▶ Maritime Security: Armed Guards on Board
- ▶ Maritime Security: Problems of Security Versus Safety Practices
- ▶ Physical Security: Best Practices
- ▶ Public-Private Partnerships: Security Organizations
- ▶ Risk Analysis: National and International Standards
- ▶ Security Management

References

Ahokas, J., & Kiiski, T. (2017). *Cybersecurity in ports*. Turku: School of Economics.

Bichou, K. (2008). *Security and risk-based models in shipping and ports: Review and critical analysis* (Discussion Paper no. 2008–20). Organisation for Economic Co-operation and Development.

Edgerton, M. A. (2013). *A practitioner's guide to effective maritime and port security*. Hoboken: Wiley.

Institute of Risk Management. *Risk appetite & tolerance guidance paper.*

International Bank for Reconstruction and Development/ The World Bank. (2009). *Supply chain security guide*.

International Organization for Standardization. *ISO/TS 22317:*2015*, Societal security-business continuity management systems-business impact analysis*.

International Organization for Standardization. *ISO 31000:*2018*, Risk management – Guidelines.*

Risk and Insurance Management Society. (2017). *2017 enterprise risk management benchmark survey.*

Sakhuja, V. (2010). *Security threats and challenges to maritime supply chains.* United Nations Institute for Disarmament Research, Disarmament Forum: Maritime Security.

United States Government. (2007). *Energy: critical infrastructure and key resources sector-specific plan as input to the National Infrastructure Protection Plan (Redacted)*. Government Printing Office.

Further Reading

Institute of Risk Management. *Risk appetite & tolerance guidance paper.*

United States Government. (2005). *The national strategy for maritime security.* Government Printing Office.

United States Government. (2009). *National infrastructure protection Plan.* Government Printing Office.

Maritime Security: Armed Guards on Board

Yarin Eski
Knowledge Hub Security and Societal Resilience/ Political Science and Public Administration, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Keywords

Maritime security · Private security guards · Weaponization · Accountability · ISPS code

Definition

Armed private security guards aboard ships protect ships and their crews against pirate attacks at sea by using nonlethal and lethal force.

Introduction

Armed private security guards on board of ships for protection against piracy have a long history. It dates back to Ancient Greece when hired groups of mariners were tasked by city-states to capture and hand over ship crews of enemy forces but also share captured booty (Ormerod 1997: 34). During the age of colonization, in particular in the sixteenth and seventeenth centuries, naval wars between rivaling colonizing European countries peaked. Governments made use of privateers (or buccaneers), which was actually a sort of licensed piracy since these privateers held a "letter of marque" from a sovereign nation to attack the sovereign's enemies (Renwick and Abbott 1999). They were considered maritime mercenaries that had their own vessel, hired and fighting for their respective governments for financial gain. The use of privateers came to a halt when governments started to use their own professional navies instead in the eighteenth and nineteenth centuries when nationalization and the building of nation-states in

Europe set in. Fast-forwarding two centuries, piracy is still and even more aggressively prevalent due to various socioeconomic problems faced by impoverished nations, such as and in particular Somalia. The Somali people endured severe drought as a result of climate change, heavy losses due to illegal fishing by foreign ships, illegal waste dumping in Somali waters, political corruption, and (ethnic) conflicts; in order to survive, there seems no other way than to generate "booty" through piracy (Beri 2011). As a response, Private Maritime Security Companies (PMSCs) entered the market, seemingly fulfilling a similar role as the privateers centuries ago. They operate not necessarily in assistance of their nations waging naval wars but rather in the protection of global shipping companies and their ships and crews against maritime terrorism and armed robbery and especially against modern piracy. This entry shall focus on the effects of PMSCs and their weaponized security guards onboard of ships against modern piracy.

Privatization and the Approach to Modern Piracy

Private Maritime Security Companies (PMSCs) are a result of the neoliberal governance mode in which the government acts from a distance as a minimalist state and lets the market fill in the governance gaps. Key for that type of governance is deregulation and privatization that restructured welfare states across the globe, letting public services be taken over by private parties as the market would function more efficiently and cost-effectively (Larner 2000).

In the maritime domain, a similar pattern has emerged. Most nations started using armed guards when governments became aware that it is not cost-effective anymore to provide their own navies (Jeffrey 2010). Simultaneously, insurance companies became more and more hesitant to pay ransom money to pirates that merely had to demonstrate that they were capable (without actually having to do it) of hijacking ships, kidnaping crews, and stealing cargo. Consequently, more responsibility was required from shipping companies in order to be eligible for being covered, and thus PMSCs are cheap solutions; however, "[r]esistance from the insurance industry is [still], however, potentially one of the primary obstacles to vessel self defense" (ibid. 512).

When PMSCs are deployed to offer protection, it occurs predominantly and most well-known, in the form of having a much cheaper group of armed private security guards on deck instead of more expensive naval forces escorting ships and ship crews through piracy-prone areas. The main difference between PMSCs and Private Military Companies (PMCs), as well as Private Security Companies (PSCs), is that PMSCs are principally sea-based and the other two mostly land-based. Still, although the sea has its unique characteristics and specific challenges, it is difficult to apply this dichotomy to all private actors in the field of maritime security, because counterpiracy can also be undertaken on land (Liss and Schneider 2015). The International Maritime Organization (IMO) speaks in terms of Privately Contracted Armed Security Personnel (PCASP), which seems to overcome that dichotomy.

Along with the privatization of public services, including protection by the state, the rise of modern piracy in the Gulf of Aden and off the Somali coastline in the early 2000s and the more recently rise of piracy-prone areas in Southeast Asia and the greater Gulf of Guinea have led to increasing costs for the shipping companies and security of their fleet at sea, turning piracy risks into high primary and secondary insurance expenses. In fact, it seems to be the case that, because of the increasing growth of piracy-prone areas, the use of PMSCs has risen drastically and heightened the competition between private maritime security providers. Consequently, that rise may have led to the fall of prices of PMSC employment; it pushes PMSCs, in order to keep a profitable business, to offer cheaper counterpiracy solutions, which could affect the quality of armed guard protection on board ships (Mudrić 2011).

It is up to flag-states to decide whether armed guards are allowed aboard their vessels or not, for which clear policies must be given, as recommended by the IMO. Given the claim that no armed ship has been taken captive by pirates, flag-states and shipping companies (as well as the

International Union of Maritime Insurance (IUMI)) are more willing to accept and have armed guards on board of ships than before. It is actually because of that claim that having armed guards on board could function solely as a preventative measure (Pizor 2012). Meaning, armed guard firing shots are actually not the main objective; their presence is enough of a deterrent. Still, in order for armed private security guards to actually be able to use their guns while obeying the law of "the flagship country, territorial waters, and ports they travel through [. . .] countries have begun to change gun laws for both the flagships and territorial waters, recognizing the need for laws allowing armed guards to utilize the legal defense of self-defense" (ibid. 549). For example, it was not until Captain Richard Phillips was kidnapped in 2009 when the United States changed their laws finally to allow armed private security guards on American ships.

Nonlethality and Trust

It is often forgotten that the actual use of fire arms by armed private security guards is usually an "ultimum remedium," a last resort, to establish robust counterpiracy measures on board. If only because using "guns may not always be necessary, particularly in incidences in which local fishermen simply approach the protected vessel out of curiosity without any malicious intent" (Liss 2007: 162). Using private security armed guard teams has become the standard solution as they assist in implementing and carrying out most of the other, unarmed, and nonlethal counterpiracy solutions based on the Best Management Practices for Protection against Somalia Based Piracy (BMP4 2011), which is one of the most important "soft law" solutions in counterpiracy practices. Also, they replace the need for having special security equipment on deck, crew counterpiracy training, armed convoys, military personnel on deck, or having to make alternative thus longer routes that altogether are not as cost-effective as having armed guards (Mudrić 2011). Furthermore, armed security guards may assist (also in ports) to prevent stowaways from entering vessels, from cargo and container theft, from drug and arms trafficking, and from terrorist attacks against ship crews (Eski 2016; Haywood and Spivak 2013).

When a team of armed guards, usually consisting of four up to five guards, is on deck, the BMP4 must be taken into account as well by that team itself. They assist the captain and ship crew in monitoring the surroundings when the ship enters a high-risk area. The physical barriers, such as razor wires and/or water cannons, are usually already put in place. The team divides itself up in certain positions, starboard and port side and back and front side. They patrol as well and also attempt to get acquainted with the crew members, if only because of instructions and giving security advice and training. The team leader and the captain and/or first officer (ought to) negotiate together what should happen in case of a piracy attack. Another important element that guarantees that armed guards are not excluded from the daily business and routines on deck is that the PMSCs are predominantly founded and staffed by ex-military or ex-law enforcement professionals (Liss 2007). The professionalism and combat experiences ease crews and give them confidence in making it through high-risk, piracy-prone areas without any harm inflicted on them. These steps of advising, negotiating, and assisting in setting up physical security effectuate that trust is created between the armed guard team and the ship crew, which is crucial in case a potentially lethal conflict situation may develop after all.

When "reasonable suspicion" arises that a ship is facing a piracy threat situation, the ship crew plus the armed guards ought to take specific recommended actions. These actions are divided in the approach stage and the attack stage (BMP4 2011). During these stages, the armed guards are not immediately allowed to engage in nonlethal, let alone lethal, firing of shots. Different nonlethal defense possibilities must be explored, such as maintaining maximum speed, following the emergency communication plan, providing ballistic protection to crew against pirates, and coursing away from approaching small boats, such as skiffs and/or so-called mother ships. In all of this, it must be absolutely sure that there are no clear visible signs of the crew being armed. The armed guards

must therefore not only be specialists in securing the perimeters but must also have expertise in identifying piracy and piratical "suspicious activity" (Symmons 2012).

Lethality, Accountability, and Profitability

If a small boat and/or a mother ship has been identified as a piracy vessel, and arms have been seen on board the vessel, it is usually based on agreements between the armed guard team leader and the captain what ought to happen in terms of firing nonlethal and lethal shots. Usually, the nearing pirates are addressed by an armed guard via a megaphone – when that does not work, warning shots are fired, and if that proves to be useless, the bow and subsequently the engine of the small boat are shot to neutralize the moving small vessel. If that does not stop the pirates, or they fireback directly at the ship and its crew, or it becomes clear an RPG rocket launcher is being prepared to fire at the ship, lethal use of force could be used by the armed guards against the small boat. Once more, also in highly dangerous, lethal situations, it is only after certain steps are taken that the armed guards may act, and also this detailed procedural process establishes trust between the captain, crew members, and the team itself.

It has happened that fishermen on skiffs have been mistaken for pirates, resulting in fishermen being wounded or even killed (Mudrić 2011). Many of these incidents seem to "remain unaccounted for, as they will most likely occur at sea and out of sight of authorities or witnesses [. . .] it is understood that if P[M]SC employees carry guns, they are also prepared to use them" (Liss 2007: 162). These incidents remain exceptional, and increasingly more attention is paid to international regulatory frameworks to control excesses of (wrongful) violence by armed private security guards, such as the International Code of Conduct for Private Security Service Providers (ICoC), several IMO Circulars, ISO 28007, as well as various nongovernmental initiatives (Liss and Schneider 2015). Still, it remains problematic that there are very limited possibilities to monitor PMSCs and deployed armed guards aboard ships who act on behalf of those PMSCs, which means that "the whole private [maritime] security system relies finally on single individuals' decisions, accountability, personality, training and performance" (Chapsos 2014: 194).

Conclusion

The existence of private actors having such availability to state-legitimized yet unchecked for coercive force seems to predominantly serve the interests of their own PMSC (comprising mostly of boosting profitability of the company) rather than those of the ship crews themselves. This perverse effect of the marketization of (maritime) security could reignite debates on (modern) privateering, as it was performed centuries ago (Gould 2017), with a focus on particularly the question of whether PMSCs are indeed as "cost-effective" if their deployment means innocent lives are taken. Those debates could be constructive for the construction of a more coherent, transnational set of collected "best (management) practices" for, in particular, education and training of private security guards in the maritime sector. Moreover, rethinking (modern) privateering could be helpful for codifying – and although problematized by the international community and maritime as well as security industries (Krahmann 2016) – specific international regulations governance of PMSCs.

Cross-References

▶ Maritime Security: Problems of Security Versus Safety Practices

References

Beri, R. (2011). Piracy in Somalia: Addressing the root causes. *Strategic Analysis, 35*(3), 452–464.

BMP4. (2011). Best management practices for protection against Somalia based piracy. Available at http://eunavfor.eu/wp-content/uploads/2013/01/bmp4-low-res_sept_5_20111.pdf.

Chapsos, I. (2014). *The privatisation of international security: The regulatory framework for private maritime security companies, using operations off Somalia, 2005–13, as a case study*. PhD Thesis, Coventry University, Coventry.

Eski, Y. (2016). *Policing, port security and crime control: An ethnography of the port Securityscape*. London: Routledge.

Gould, A. (2017). Global assemblages and counter-piracy: Public and private in maritime policing. *Policing and Society, 27*(4), 408–418.

Haywood, R., & Spivak, R. (2013). *Maritime piracy*. London: Routledge.

Jeffrey, R. S. (2010). An efficient solution in a time of economic hardship: The right to keep and bear arms in self-defense against pirates. *Journal of Maritime Law & Commerce, 41*, 507–540.

Krahmann, E. (2016). Choice, voice, and exit: Consumer power and the self-regulation of the private security industry. *European Journal of International Security, 1*(1), 27–48.

Larner, W. (2000). Neo-liberalism: Policy, ideology, governmentality. *Studies in Political Economy, 63*, 5–25.

Liss, C. (2007). The privatisation of maritime security-maritime security in Southeast Asia: Between a rock and a hard place? In T. Jäger & G. Kümmel (Eds.), *Private military and security companies* (pp. 135–148). Wiesbaden: VS Verlag.

Liss, C., & Schneider, P. (2015). Regulating private maritime security providers. *Ocean Development & International Law, 46*(2), 81–83.

Mudrić, M. (2011). Armed guards on vessels: Insurance and liability. *Poredbeno Pomorsko Pravo, 50*(165), 217–268.

Ormerod, H. A. (1997). *Piracy in the ancient world*. Baltimore: JHU Press.

Pizor, B. E. (2012). Lending an invisible hand to the navy: Armed guards as a free market assistance to defeating piracy. *Case Western Reserve Journal of International Law, 45*(2012), 545–578.

Ralby, I. (2018). What went wrong when regulating private maritime security companies. In *Operational law in International Straits and current maritime security challenges* (pp. 161–180). Cham: Springer.

Renwick, N., & Abbott, J. (1999). Piratical violence and maritime security in Southeast Asia. *Security Dialogue, 30*(2), 183–196.

Symmons, C. R. (2012). Embarking vessel protection detachments and private armed guards on board commercial vessels: International legal consequences and problems under the law of the sea. *Military Law and the Law of War Review, 51*, 21.

Further Reading

Chapsos, I., & Kitchen, C. (Eds.). (2015). *Strengthening maritime security through cooperation* (Vol. 122). Amsterdam: IOS Press.

Cullen, P., & Berube, C. (Eds.). (2012). *Maritime private security: Market responses to piracy, terrorism and waterborne security risks in the 21st century*. London: Routledge.

Maritime Security: Contraband

John M. Jelenek
Security Department, NewYork-Presbyterian Hospital, New York, NY, USA

Keywords

Contraband · Coordination · Interdiction · ISPS Code · Public-private partnership

Definition

Maritime security in this context refers to the standardization and bolstering of efforts across agencies and governmental administrations to increase efficiency in the prevention of illicit smuggling activities and capturing illegal material before it makes land fall (International Maritime Organization/IMO 2019).

Introduction

In the pre- and post-9/11 years, US maritime and port security has taken a strong stance on the physical mitigation, prevention, and preparedness in regard to occurrences at seaports, arguably the most vital economic vein for the USA and the world. Despite millions of dollars having been invested in security operations at the various ports across the USA, known drug smuggling operations through maritime avenues have gone relatively unhindered. Two main reasons for this problem are a lack of coordination between public and private law enforcement personnel at the seaports and a nonexistent standard of training for

the private personnel that relies almost solely on recommendations (International Maritime Organization & International Labor Organization 2003). Efforts to address these issues included the passage of the Maritime Transportation Security Act, which effectively transferred control of US maritime security operations to the Department of Homeland Security and the Transportation Worker Identification Credential Program and Container Security Initiative, which bolstered the strong stance on protecting the homeland from seaborne terrorist attacks via CBRNE weapon usage (CBO 2016; CRS Report 2005; Leonard et al. 2015; Nemeth 2017b). However, detection, screening, and intelligence programs gauged toward the war on contraband have gone relatively unchanged since the late 1990s.

An active and consistent threat with significant impact seen across the USA is the use of cargo containers to smuggle illicit material through established maritime routes to seaports and onto US soil. Success in this type of operation by transcontinental criminal organizations is widespread as shipping hubs on all coasts are targets (CIA World Fact Book 2019). Being a worldwide phenomenon, drug smuggling is not limited to any sole group, and the demographics of the people involved will change depending on the region(s) in which the cargo is leaving and entering. The tactic of using and embedding illicit material within cargo containers was implemented in the 1990s and is still used due to three facts. First, screening methodologies focus almost solely on CBRNE threats (Nemeth 2017b). Second, financial loss due to slow processing has encouraged a pattern of rushed screening of containers; specifically, out of the near 12 million containers reaching the USA annually, roughly only 600,000, or 5%, are screened and searched (CBO 2016). Third, there is an evident lack of joint training and communication between the Customs and Border Protection (CBP), US Coast Guard, and their private law enforcement counterparts stationed at these ports. The only mention of cooperation is with foreign government agencies with a similar role (CBP 2019). There is no information on the training requirements for port security contractors beyond a list of courses provided by licensed training providers and the standards established by the US government through the National Maritime Transportation Security Plan (Cornell Legal Information Institute), leaving a relatively blank slate to reform and build off of current policies and directives in order to create a comprehensive and standardized training program with fluid communication between public and private law enforcement officers being paramount.

Offender Demographics and Methodology

In order to build a comprehensive policy not only applicable to the USA, but globally, this section will provide an overview of the demographics of offenders; current security procedures in place for mitigation and prevention; the private-public partnership, both in its triumphs and shortfalls; and areas in which improvements can be made. The reality of our interconnected world, which thrives on trade from all over the globe, is that groups in various locations and of various backgrounds are able to take advantage of this security void for their own devious operations. In the case of drug smuggling operations involving maritime methodologies, there are specific groups who have the most activity. Due to their proximity to the USA, people of Afro-Carib, Amerindian, and Hispanic descent from areas, such as Jamaica, Dominican Republic, Cuba, Mexico, Colombia, and Haiti, ranging in age from adolescence to late adulthood, are the most prevalent in smuggling marijuana, cocaine, and heroin to the Atlantic Coast (Department of Justice 2011, pp. 15 & 16; Department of Justice 2015, pp. 1–4; Department of Justice 2016, pp. 6, 10 & 14). This age gap depends on the length of time of the person's affiliation with the criminal organization and also reflects the reality that people of all ages will take part in these activities in order to support themselves or their families. For operations on the Pacific Coast, people of Asian descent are most often involved in smuggling (Department of Justice 2015, p. 6;

Department of Justice 2016, p. 16) and predominantly supply purified ecstasy, known as MDMA, and smaller amounts of crystal methamphetamine (Department of Justice 2015, p. 7). Fentanyl, a highly toxic synthetic opioid, and its precursor chemicals have also joined the list in the past several years. In regard to the age of perpetrators of Asian descent, they also range in age.

The motives behind the offenses performed by those engaging in smuggling activities have been and are currently based completely in profitability. Drug trafficking, counterfeit goods, gun running, and human trafficking are ideal money-making opportunities for criminal organizations and illegal businesses, especially in a market as large as the USA. As of 2010, a White House report estimated nearly $109 billion was spent on narcotics in the USA alone; this number had gone virtually unchanged since a similar 2000 report (Business Insider 2016).

The main method in which illicit drugs enter the US homeland through maritime routes is through the commissioning of private vessels ranging from small outboard engine vessels to submarine-type craft to be used as runner boats. The idea is to move quickly, traveling from point to point without raising suspicion or drawing too much attention. This method, popularized by South American cartels such as the Sinaloa, has proven to be successful, but it does not directly involve major US seaports as drop zones are usually in discreet locations along the coastline of the Southern USA (Department of Justice 2017). Alternatively, cruise ships and ferries have also been utilized as another form of product transport, predominantly in southern Atlantic ports and in Gulf Coast ports. Lastly, commercial ships, specifically container transporting vessels, have become a key asset to transcontinental criminal organizations (Department of Justice 2010). The use of these benign behemoths is the newest and the most discreet mode of transport as copious amounts of the chosen payload can be stored among the immense number of cargo containers, among cargo and provisions deemed necessary for successful voyage, or among typical carry-on luggage of the personnel on board (IMO 2017). For operations involving cargo ships, the crew members are considered to be main smuggling suspects as many of the personnel, especially coming from South America, are usually involved with the trafficking organization. The increased favoring by smugglers for commercial container transports has been due to their size, known lack of screening, and, as stated before, ability to involve the crew of the vessel (Department of Justice 2011, pp. 15 & 16). As of 2009, the estimated worldwide total of shipping containers used yearly to transport over 90% of worldwide goods from point to point was approximately 420 million (UNODC 2009); however, the current estimated total of all shipping containers in the world sits at upwards of 35 million units (World Shipping Council 2017 & *Container Supply Review: May 2011* 2011, p. 3).

Security Procedures

It is a ceaseless task to secure US and global seaports alike as the cargo entering them each day and the list of procedures and stakeholders involved are constantly growing and changing. Following the creation of and consolidation of agencies under the Office and Department of Homeland Security in 2001, maritime operations became a necessary and costly, yet effective, investment. The same is to be said for the private sector involved in maritime operations. In fiscal year 2017, an estimated $2.3 billion of the total DHS budget went to marine operations (DHS 2017, pp. 4 & 5) involved with securing ports and the interdiction of drug and general smuggling personnel and paraphernalia.

Positive procedures for security and interdiction have developed from multiple national and international agencies and departments such as the US Customs and Border Protection's requirement and partnering with businesses to form standards of screening their shipping employees and personnel, listing of all parties involved with the contents of containers and cargo, and the thorough inspection of containers heading to US ports (CBP, Security Profile for Businesses & CBP 2009); the creation of the International Maritime Organization's ISPS, or International Ship and

Port Facility Security Code, in 2002 and its update in July 2014 to standardize and bolster current international risk management and security procedures (International Maritime Organization 2017 & International Maritime Security Organization 2017, FAQs); the US Coast Guard's training and development programs for container security and interdiction (Nemeth 2017b, pp. 421 & 422); and the United Nations Office on Drugs and Crime's Global Maritime Crime Programme, which helps to train law enforcement and military units throughout the world on tactics and procedures for capturing and preventing drug smuggling and terrorist activity at sea and at ports worldwide while also properly investigating and fully prosecuting these actors (UNODC 2016, pp. 4 & 5). US-born security implementations in conjunction with international standards and procedures create awareness throughout the world's governments and private sector organizations, fostering communication and cooperation while successfully apprehending suspects around in all bodies of water from the Atlantic Ocean to the Strait of Hormuz (Nemeth 2017b, p. 427; U.S. Coast Guard 2015; UNODC 2016, pp. 11–24).

Although there are positive procedures and initiatives that have proven to be effective, there are still those remaining which have done little to aid in the worldwide fight against maritime drug smuggling. The current training of those involved with large cargo or people-carrying ships, as well as ports, is lacking in many areas. Classroom-style training geared toward securing the port cannot substantially display the situations the port officers will find themselves in as they will become functional search units for containers that have been flagged. Combining a lack of training, restricted searches to flagged containers of interest, and an inability to screen the flagged containers and ships alike thoroughly within a set time frame can lead to an endless cycle of illicit items "slipping through the cracks."

Companies and stakeholders in general in the USA adhere to the 2002 Maritime Transportation Security Act and to the ISPS Code when in international waters, but there is little specificity or acknowledgment of training length for personnel involved in maritime security. The 46 US Code § 70125 simply outlines the topics that port security officers must be trained and proficient in as well as which companies are licensed to train; however, this goes without mention of a standardized training time frame (United States Government 2010). Companies ranging from Academi to DNVGL vary their training from a few days to a full week or more, presenting their courses in different manners for different maritime situations. This lack of congruency comes with the issues of security personnel being trained to varying proficiency levels in monitoring and response efforts for hostile situations or suspicious activity and in the proper methods of searching cargo containers for tampering or contraband presence (United States Government 2010).

Public and Private Stakeholders

The public agencies directly involved in the task of maritime and port security are the US Customs and Border Protection and the US Coast Guard as they directly make arrests, conduct searches and seizures, and ensure that ships, containers, and crew members are compliant with US code (Nemeth 2017b, p. 436). However, in the case of illicit drug smuggling, many other peripheral and cooperative agencies are also involved due to the landfall of copious amounts of these substances. The FBI, DEA, NYPD and their Regional Intelligence Center, and local law enforcement agencies (Department of Justice 2008) across the USA with jurisdiction in areas with seaports play crucial roles in intelligence acquisitions, investigations, and arrests in regard to the drug trade and the people involved.

Port security breaches in regard to drug smuggling and the responses elicited after a breach are few due to the nature of these breaches occurring often and without realization. The breach tends to be found once the substances have made it to their final destination and hit the street for distribution. There is no information on concrete response methods used by either sector (CBP 2017a, b). One can assume that following an apprehension and

investigation involving illicit drugs, information yielded about how the drugs arrived in the country would be dispersed to all other public agencies and then to the private companies providing security and screening operations at these ports. A tightening down of operations would be the logical response. One of the disheartening factors in this is that the National Incident Management System and Incident Command System, as well as their corresponding National Response Framework, are not used for drug intelligence and incident response (FEMA 2008, 2013). The only mitigation and coordination currently underway directly involving the private and public sectors are through interdiction and screening; screening has been the least effective as most programs initiated by the USA for global use focus on CBRNE threats at seaports, such as with the CBP's Container Security Initiative, the C-TPAT, Maritime Transportation System Security Plan, and the National Strategy for Maritime Security (Nemeth 2017a, pp. 377, 379, 419 & 421).

Coordination methods, as stated before, do not thoroughly deal with or mention drug trafficking and smuggling. Coast Guard interdictions at sea and law enforcement operations on land have yielded the highest removal of narcotics as well as the production of intelligence (Coast Guard Compass 2017) while also leaving the private sector virtually in the dark and in a state of proverbial business as usual. With an obvious lack in coordination methods for incident response and mitigation, likelihood of success by the actors only increases.

Opportunities for Improvement

The spotlight of maritime security procedures and technology development has been on the prevention of terrorism and possible attacks, creating a lack of focus on the illicit drug trade and its involvement of US and international seaports and waterways. Increased training, stricter requirements of new hires, increased coordination between private and public organizations, increased port security officer salaries, and better detection methods such as the use of drug-sniffing canine units are the most viable options fiscally and operationally that can be executed with relative ease (CBP 2019; IMO 2003).

Public agency-sponsored training has reflected a lack in drug indictment training for private sector members of security operations. The proof of this is in over 20,000 drug-related cases in which a majority was trafficking related, a substantial portion coming from maritime avenues of initial delivery (USSC 2015, p. 6). With the exception of the Coast Guard's boarding exercises and proficiency among its proprietary personnel, seaport practice events organized by the Coast Guard that also include private guard forces do not reference or deal with the finding of drugs and associated paraphernalia on personnel or within cargo containers (Nemeth 2017b, p. 430) and instead focus on explosive ordinance disposal and similar threats from unidentified and suspicious maritime and land vehicles (Book of Maritime Security Exercises, Appendix 5-1 through 5-4). Deficiencies are found across the board from access control measures to the requirements of drills (Nemeth 2017b, Fig. 10.34), an unacceptable reality that can be fixed with the use of knowledge through experience, information, and incentive. By increasing the information and intelligence flow to the private contracted personnel providing supplementary security and law enforcement at seaports, targeted containers and ships of interest can be held and their contents sifted through with supervised expertise. Agency-sponsored standardized training used to create congruency in the abilities of Coast Guard and port security officers will put the information to use in an efficient way and bolster the currently implemented Container Inspection Training and Assist Team (Nemeth 2017b, p. 432). Another inherent benefit to this is the utilization of the ability of probable cause of the security officers (United States v. Day; Nemeth 2017b, p. 434) to search these vessels and containers in question. While considered a legally questionable action by some, it can improve the ability to intercept illicit drugs before they hit the mainland by bypassing typical conduct and search and seizure legalities public law enforcement officers must adhere to.

With increased information, there potentially is a risk of issues in trustworthiness and

competence. Strong vetting procedures similar to that of the requirements to obtain a governmental secret clearance and increased standards for required education and experience help mitigate this problem (CBP 2019; IMO 2003). An established history of the candidate or current security officer will remove questionable personnel, and an education specializing in law enforcement, homeland security, or security operations makes them more attractive as a member of the public-private team.

The long fought and ongoing battle in the private security industry in regard to compensation cannot be avoided in this sector of operations. The US Department of Justice notes that coordination is essential to a successful drug smuggling operation and at times those who clear and handle cargo are on the payroll of a trafficking organization (Department of Justice 2015); this does not exclude security personnel. Although a broad representation over multiple focuses within the security industry, as of May 2016, the Bureau of Labor Statistics' (2017) data shows that the average security officer earns roughly $25,000 per year or $12 per hour. When compared to their Coast Guard counterparts, the disparity is noticeable as officers are paid at a GS-5 or higher pay grade and Specialists outearn both of these, doubling their salary. By improving pay, the desire to break the law in order to earn extra money is reduced, and quality of work and employee loyalty will rise.

Bolstering the human end of these operations, canine units and their superior natural detection through scent have proven invaluable through use by law enforcement worldwide. For seaport drug detection, the German shepherd breed would prove most useful as they have the highest average percent of detection of a range of drugs at around 80% (Jezierski et al. 2014). These animals have been widely used and have successfully located hidden drugs at land-based ports of entry, leading to arrests and seizures of illicit substances with monetary street value in the millions (CBP, Pharr Int'l 2017a; CBP, Laredo 2017b). By investing in the training of handlers and dogs, targeted containers and ships can be thoroughly swept beyond what a human can achieve. In addition to this, the ability to cover a larger area of the port and increased number of containers that may have not been flagged will boost operational efficiency. The cost of training, averaging at approximately $3,000 per dog and $5,000 per handler (Coutts, Cost of a Canine Program n.d.), plus necessities and upkeep, will have a guaranteed exponential return on the original investment when a small team is formed.

Conclusion

Through the increased training and coordination of public and private entities tasked with the security operations of maritime and seaport assets and the interdiction of illicit drugs, the assumed effect is that there will be a decrease in the quantity of these substances making their way to the global street market. By removing the accessibility to these substances, public health will increase as addiction rates and communicable diseases related to the paraphernalia used decline and mortality rates from drug overdoses decrease. In 2016, there were over 60,000 fatal drug overdoses in the USA alone; a 20% increase since 2015. It is estimated that nearly 21 million Americans have an illegal substance abuse problem (ASAM 2016; NIDA, Heroin 2017a; NIDA, Overdose Death Rates 2017b). As for security operations at seaports, standardized communication and training for the private and public organization personnel involved will lead to a well-rounded operation filling the vulnerabilities that were once commonplace, tightening down on what can be considered as acceptable risk, and establishing a standard that other nations can build and improve their own operation procedures upon.

Cross-References

- ▶ Maritime Security: Acceptable Risks
- ▶ Maritime Security: Armed Guards on Board
- ▶ Maritime Security: Problems of Security Versus Safety Practices

References

46 U.S. Code § 70125 – Port Security Training for Facility Security Officers. (2010, December). Washington, DC: U.S. Government. Retrieved 10 July 2019, from https://www.law.cornell.edu/uscode/text/4

CIA World Factbook. Retrieved 10 July 2019., from https://www.cia.gov/library/publications/the-world-factbook/fields/2120.html

Coutts, J. (n.d.). *Costs of a Canine Program across the United States* [Scholarly project]. American Society of Canine Trainers. Retrieved 30 July 2019, from http://asctk9.org/sitebuildercontent/sitebuilderfiles/JasonCouttsPDF.pdf

Customs and Border Protection, Department of Homeland Security. (2017a, October 4). CBP Officers from the Pharr International Bridge Seize Over $4 Million in Narcotics [Press release]. Retrieved 14 July 2019, from https://www.cbp.gov/newsroom/local-media-release/cbp-officers-pharr-international-bridge-seize-over-4-million-narcotics

Customs and Border Protection, Department of Homeland Security. (2017b, October 23). CBP Officers Seize More Than $1.7 Million in Crystal Methamphetamine at the Laredo Port of Entry [Press release]. Retrieved 17 July 2019, from https://www.cbp.gov/newsroom/local-media-release/cbp-officers-seize-more-17-million-crystal-methamphetamine-laredo-port

Customs and Border Protection, Department of Homeland Security CSI: Container Security Initiative. (2019, May 31). Retrieved 8 Nov 2019, from https://www.cbp.gov/border-security/ports-entry/cargo-security/csi/csi-brief

Frittelli, J. F. (2005). *CRS Report for Congress Port and Maritime Security: Background and Issues for Congress* (United States, Congressional Research Service, U.S. Congress). Washington, DC: U.S. Government.

International Maritime Organization. (2019). Our Work: Maritime Security and Piracy. Retrieved 30 Dec 2019, from http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx

International Maritime Organization & International Labor Organization. (2003). *Code of Practice on Security in Ports*. Geneva: IMO.

Jezierski, T., et al. (2014). Efficacy of drug detection by fully-trained police dogs varies by breed, training level, type of drug and search environment. *Forensic Science International, 237*, 112–118. Retrieved 12 July 2019.

Leonard, T. J., Gallo, P., & Veronneau, S. (2015, March 3). *Security Challenges in United States Sea Ports: An overview*. New York: Springer Science Business Media. Retrieved 12 July 2019.

National Institute on Drug Abuse. (2017a, July). Drug Facts: Heroin. Retrieved 15 Aug 2019, from https://www.drugabuse.gov/publications/drugfacts/heroin

National Institute on Drug Abuse. (2017b, September). Overdose Death Rates. Retrieved 15 Aug 2019 from https://www.drugabuse.gov/related-topics/trends-statistics/overdose-death-rates

Nemeth, C. P. (2017a). Chapter 9: Border security, U.S. citizenship, and immigration services. In *Homeland security: An introduction to principles and practice* (3rd ed., pp. 359–395). Boca Raton: CRC Press.

Nemeth, C. P. (2017b). Chapter 10: Transportation and security. In *Homeland security: An introduction to principles and practice* (3rd ed., pp. 397–462). Boca Raton: CRC Press.

United States, Drug Enforcement Administration, Department of Justice. (2011). *National Drug Threat Assessment 2011*. Washington, DC: U.S. Government.

United States, Drug Enforcement Administration, Department of Justice. (2015). *National Drug Threat Assessment 2015*. Washington, DC: U.S. Government.

United States, National Drug Intelligence Center, Department of Justice. (2008, June). *New York/New Jersey High Intensity Drug Trafficking Area Drug Market Analysis 2008*.

Further Reading

International Maritime Organization. (2016). *Guidance for the development of national maritime security legislation*. London: United Nations.

International Maritime Organization. (2017a). *International Ship and Port Facility Security (ISPS) Code*. Retrieved 12 July 2019, from http://www.imo.org/blast/mainframe.asp?topic_id=897

International Maritime Organization. (2017b). *Maritime Security and Piracy Security.*

Security Guards and Gaming Surveillance Officers. (2016, May). Retrieved 22 July 2019, from https://www.bls.gov/ooh/protective-service/security-guards.htm

United Nations, Office on Drugs and Crime. (2016). *Global Maritime Crime Programme: Annual Report 2016*. Nairobi: United Nations.

United States, Coast Guard, Department of Homeland Security. (n.d.). *Book of maritime security exercises E2 – Port facility exercises Part 1: Guidelines for the planning and conduct of maritime security exercises*. Washington, DC: U.S. Government.

United States, Coast Guard, Department of Homeland Security. (2019). *Navigation and vessel inspection circular NO. 09-02, change 5*. Washington, DC: U.S. Government.

United States, Congressional Budget Office, U.S. Congress. (2016, June). *Scanning and imaging shipping containers overseas: costs and alternatives*.

United States, Customs and Border Protection, Department of Homeland Security. (2009). *Importer security filing and additional carrier requirements*. Washington, DC: U.S. Government.

United States, Department of Homeland Security. (2017). *FY 2017 Budget in Brief*. Washington, DC: U.S. Government.

United States, Drug Enforcement Administration, Department of Justice. (2016a). *National Drug Threat Assessment 2016*. Washington, DC: U.S. Government.

United States, Drug Enforcement Administration, Department of Justice. (2016b). *National Drug Threat Assessment 2017*. Washington, DC: U.S. Government.

United States, Government Accountability Office. (2008). *Supply chain security: Examinations of high-risk cargo at foreign seaports have increased, but improved data collection and performance measures are needed*. Washington, DC: BiblioGov Project.
United States, Federal Emergency Management Agency, Department of Homeland Security. (2008). *National Incident Management System*. Washington, DC: U.S. Government.
United States, Federal Emergency Management Agency, Department of Homeland Security. (2013). *National Incident Management System: Intelligence/investigations function guidance and field operations guide*. Washington, DC: U.S. Government.
Woody, C. (2016, March 16). NARCONOMICS: The real drugs millionaires are right here in the United States. Retrieved 14 July 2019, from http://www.businessinsider.com/where-drug-money-goes-2016-3

Maritime Security: Problems of Security Versus Safety Practices

Yarin Eski
Knowledge Hub Security and Societal Resilience/Political Science and Public Administration, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Keywords
Maritime safety · Maritime security · Resilience · ISPS Code · SOLAS

Definition

Overall, maritime safety encompasses the protection of ports, ships, and their communities against unintentional dangers and harms (e.g., storm at sea), whereas maritime security encompasses the protection of ports, ships, and their communities against deliberate dangers and harms (e.g., piracy). The two can be complementary or conflicting.

Introduction

The safety versus security debate is persistent in any professional domain, whether that is in agriculture, policing, education, or IT (Line et al. 2006), and thus in the maritime industry as well. Overall, "[t]he inability of the system to affect its environment in an undesirable way is usually called safety; the inability of the environment to affect the system in an undesirable way is usually called security" (ibid. 1). However, depending on the environments and systems themselves, as well as the damaging effects they can both have on each other, there can be numerous definitions of safety and security. The maritime safety versus security divide (if a divide at all) resembles the divide in other domains and is similar to the (definitional) issues that come along with it:

> Maritime safety accidents are unintentional, while maritime security and piracy incidents are intentional. Maritime and piracy incidents differ in that the focus of the forms is damage to property and/or injury to individuals for political reasons while that of the latter is theft. Maritime safety accidents, security incidents and piracy incidents, however, may have the same outcomes – injuries and property damage. (Talley 2013, p. 1)

For a long time, the focus of ships was predominantly on safety, given the daily concerns of being at sea (e.g., sea storms, ship damage, etc.), which changed drastically after 9/11 but not easily resolved, as security required almost the opposite acts and equipment to the need for safety.

In this entry, key issues in the maritime safety versus security debates, and where problems may arise, shall be explored by giving a concise overview of the International Convention for the *Safety* of Life at Sea (SOLAS) and the International Ship and Port Facility *Security* Code (ISPS Code). Furthermore, this entry explores the conceptual and practical ambiguity of maritime safety and security in the everyday of the maritime industry.

Maritime Safety: SOLAS

SOLAS is an immediate legislative response to the sinking of the Titanic in 1912. It came into force in 1914 and brought about new obligations for particular ships to comply with, such as a minimum number of lifeboats and obligated specific safety equipment (Eski and Carpenter 2013).

Ever since, SOLAS received many amendments, especially in the twentieth century. The Inter-Governmental Maritime Consultative Organization (IMCO), which has become the International Maritime Organization (IMO) since 1982, is the official body to deliver and update legislation for ships and ports to comply with SOLAS (ibid.). Several key topics are covered under maritime safety, including carriage of cargoes and containers, fire protection, navigation, radio communications and search and rescue, stability and subdivision, and the international and national safety regulations themselves (IMO 2018).

These days, the term "maritime safety culture" has gained popularity and is heavily promoted throughout the maritime industry by the IMO (Ek et al. 2014). The following is stated by the IMO on safety culture:

> An organization with a 'safety culture' is one that gives appropriate priority to safety and realizes that safety has to be managed like other areas of the business. For the shipping industry, it is in the professionalism of seafarers that the safety culture must take root. (IMO 2012)

There is, however, no homogenous maritime safety culture, because the professionalism that is required of maritime professionals in ports and on ships "is determined by attitudes and performance, very often shaped by the culture of the shipping company" (Ek et al. 2014, p. 180), and these can differ also in maritime security practices and culture.

Maritime Security: ISPS Code

A major amendment to SOLAS was the addition of a new Chapter "Special Measures to Enhance Maritime Security", following a Conference of Contracting Governments to the Convention that was held in London in December 2002. It was done so due to the Twin Towers attacks which amplified security awareness significantly in the maritime industry, requiring, predominantly:

> . . .the installation of automatic identification systems on ships, the need for security plans for ships, port facilities and off-shore terminals, the need to verify the identity of seafarers and the question of a secure 'chain of custody' for containers from their port of origin to their destination. (Von Hoesslin 2005, p. 1336)

Codifying the identified needs, the International Ship and Port Facility Security (ISPS) Code (IMO 2003) entered the maritime industry. It identifies and intensifies cooperation between a wide variety of public and private partners, ranging from the police to customs, to security companies and port authorities, all working together through multi-agency partnerships, in the name of "maritime security" to tackle, first and foremost, terrorism and maritime-related crime, such as drug trafficking, human smuggling, and cargo and container theft. The Code also aims to harmonize interpretation and implementation of SOLAS Chapter "Special Measures to Enhance Maritime Security", and the ISPS Code throughout the world, as well as enabling the cooperating public-private maritime security and policing institutions to share information with each other, nationally and internationally. The Code has brought major differences to the maritime industry, in particular in regard to physical security, turning the once open port territory to an international zone that is closed off from the main public. It also introduced new roles which ships and ports had to fulfill as of 1 July 2004.

The ISPS Code consists of a mandatory part A that lists security obligations which ships and ports must be in compliance with and a recommendatory part B, although the part B provisions are practically as mandatory as part A is (Kim and Lee 2013, p. 283). The ISPS Code aims to standardize the evaluation of security risks and to make sure that all ships and ports, in interaction with each other, "perceive and manage security threats through integrating local/domestic threat-levels into a global awareness-level" (Bichou 2004, p. 328). Still, there is room in the ISPS Code for variations in ship and port security settings (IMO 2003), as long as measures taken cause minimum interference to daily transport activities.

In line with standardization, new official security roles are mentioned that must be present (whereas official safety roles are not as clearly described), such as the ship security officer (SSO), the port (facility) security officer (P(F)SO), and a designated authority (DA). Moreover,

there are different official documents, such as the Declaration of Security (DoS) that is established between the SSO and PFSO, or the Ship Security Plan/Port Facility Security Plan (SSP/PFSP), and the Ship Security Assessment/Port Facility Security Assessment (SSA/PFSA) that must be designed and approved for each ship and facility. These roles and documents ought to guarantee continuous development of maritime security (harmonization) through the identification of (threats to) critical infrastructure and any weaknesses in the maritime industry.

Maritime Safety Versus Maritime Security: Conceptual and Practical Ambiguity

English is the maritime language, and thus, naturally, there is the complexity of different linguistic understandings of maritime security and safety (McNicholas 2016). Take, for example, the German "Sicherheit" (which could mean, next to safety and security, also certainty) or the Hebrew "bitachon" (which means security but also trust and faith) or the Dutch "veiligheid" (which means safety as well as security). Meaning differences between "security" and "safety" do not always exist linguistically; there can be more meanings of the words. Non-native English-speaking maritime professionals are thus forced to take over the English terminology, which may cause communication issues, thus leading to different understandings and practices of maritime safety and security.

There are many more aspects leading to conceptual and practical ambiguity, even rivalry, between maritime security and safety. Given the long existence of SOLAS as international maritime safety legislation and the, in comparison with SOLAS, short existence of the ISPS Code, the current generations of maritime professionals are automatically more maritime *security* focused, whereas previous generations have been more maritime *safety* focused.

Maritime security logic has dominated the maritime industry since 9/11 and two attacks on US naval destroyers in 2000, the *USS The Sullivans* and the *USS Cole*, of which the latter was claimed by al-Qaeda (Metaparti 2010). Maritime security through the ISPS Code and its new security roles and rigid bureaucracy (Liss 2011) has been in particular focused on counterterrorism, shifting the focus in the maritime industry from safety to security and making it seem as if security practices surpass safety practices.

Practically though, maritime safety still matters in everyday maritime professional life. Shipping crews, port workers, and the overall maritime professional population seem to have more safety awareness than security awareness as safety awareness is more naturally adapted to and thus more integrated into daily routine to effectively *support* daily routine. Maritime safety (awareness) appears more important as well because maritime security (awareness) is not as much a part of the daily routine as safety is: maritime terrorist attacks, the main focus of the ISPS Code, barely happen (Metaparti 2010). However, occupational hazards occur far more frequently, leading to safety awareness being significantly more integrated into daily routine, reflected in having to wear personal protection equipment (PPE), holding onto bars, and being careful with dangerous goods – security threats such as piracy, drug crime, or terrorism are far more invisible and rather alien to maritime workers, also security workers, in ports and on deck, resulting in professionals not taking maritime security (awareness) as seriously as maritime safety (awareness) (Eski 2016).

Moreover, "What is maritime security?" as Bueger (2015) wonders. It is not as established as maritime safety but still "replaces or subsumes older, established concepts, as well as relates to more recently developed ones," namely, "sea power, marine safety, blue economy, and human resilience" (ibid. 160). It indicates that safety is a part of maritime security, which is not necessarily experienced by the professionals in the maritime industry, leaving "maritime security" behind as a buzzword with no definite meaning, and it merely "achieves its meaning by actors relating the concept to others, by attempts to fill it with different issues and by acting in the name of it" while "vary[ing] across actors, time, and space" (ibid. 163).

On top of it, the ambiguity of the two apparently different concepts can also blur both their practices, which further complicates operational realities on deck and at the docks. Right after the financial crisis and austerity policies hit port communities throughout the world, in particular from 2010 onward, port workers feared losing their job, not being able to sleep, while having to handle containers in cranes and vessel carriers for which they must be focused and awake and must comply with strict regimes regarding their working hours (Eski 2016). Due to the same fear of losing one's job, these employees as "safety risks" can also become "security threats" because they might steal something or turn corrupt and assist criminal organizations that run illegal drug trafficking operations in ports (Eski and Buijt 2016). Both challenges must be dealt with security personnel, usually through different norms and rules; however, in reality, time and context can blur being a "safety risk" and/or "security threat" which may undermine maritime logistics (Cowen 2007).

The "safety risks" and "security threats" blur as well due to the ISPS Code's focus on (counter) terrorism. Sometimes, it demands that entries must be closed and secured, but due to safety regulation revolving around fire hazard, these points of access ought to remain open. At a petrochemical port facility, when an oil tanker is anchored, (extra) escape gangways are required to escape from a fire on board, but this conflicts with ISPS Code regulation regarding gangways, as (extra) entries means having more possibilities for outsiders and threats to enter a ship. Or think of the doors of a port facility being locked to minimize the security risk of cargo theft, but must be opened as soon as a chemical gas of a dangerous good spreads itself. What prevails? Security or safety? Or consider SSOs and PFSOs who take care of both safety-related issues, such as applying first aid, and of security issues, like stopping unauthorized individuals from entering a ship and/or a port facility. When letting authorities, such as the police or customs agencies, enter port facilities and ships to do security inspections, due to the principle of "safety first" and the different safety measures on board and on facility perimeters, these authorities are forced by an SSO or PFSO to wear personal protection equipment (PPE). It happens occasionally that the police and border control authorities that are tasked to keep a port secure are aggravated by and get into a conflict with PFSOs and SSOs who demand compliance with safety rules.

Conclusion

In conclusion, although the ISPS Code symbolically prioritizes the unclear concept and practices of maritime security over maritime safety, it is important to account for maritime safety practices as still being (much more) common in the everyday of the maritime industry. At the very least, there seems to be conceptual and practical ambiguity *between* and *because* of the two, which leads to rivalry at operational level that could result in serious damages (Knapp and Franses 2010). It could be interesting to have the two concepts integrated, without ignoring their (different) real effects, into what is being increasingly developed a framework of maritime resilience (Sauser et al. 2018).

M

Cross-References

▶ Maritime Security: Armed Guards on Board

References

Bichou, K. (2004). The ISPS code and the cost of port compliance: An initial logistics and supply chain framework for port security assessment and management. *Maritime Economics & Logistics, 6*(4), 322–348.

Bueger, C. (2015). What is maritime security? *Marine Policy, 53*, 159–164.

Cowen, D. (2007). Struggling with 'security': National security and labour in the ports. *Just Labour: A Canadian Journal of Work and Society, 10*, 30–44.

Ek, Å., Runefors, M., & Borell, J. (2014). Relationships between safety culture aspects–A work process to enable interpretation. *Marine Policy, 44*, 179–186.

Eski, Y. (2016). *Policing, port security and crime control: An ethnography of the port securityscape*. London: Routledge.

Eski, Y., & Buijt, R. (2016). Dockers in drugs: Policing the illegal drug trade and port employee corruption in the

port of Rotterdam. *Policing: A Journal of Policy and Practice, 11*(4), 371–386.
Eski, Y., & Carpenter, A. (2013). Policing in EU seaports: Impact of the ISPS Code on Port Security Post-9/11. In M. O'Neill, K. Swinton, & A. Winter (Eds.), *New challenges for the EU internal security strategy.* Newcastle upon Tyne: Cambridge Scholars Publishing.
IMO. (2003). *ISPS Code*. London: IMO.
IMO. (2012). Safety cultures. Available at: http://www.imo.org/OurWork/HumanElement/SafetyCulture/Pages/Default.aspx
IMO. (2018). Maritime safety. Available at: http://www.imo.org/en/OurWork/Safety/Pages/Default.aspx
Kim, S. K., & Lee, S. (2013). The legal framework of maritime security in East Asia: A comparative view. In H. N. Scheiber & J. H. Paik (Eds.), *Regions, institutions, and law of the sea: Studies in ocean governance* (pp. 271–292). Leiden: Martinus Nijhoff Publishers.
Knapp, S., & Franses, P. H. (2010). Comprehensive review of the maritime safety regimes: Present status and recommendations for improvements. *Transport Reviews, 30*(2), 241–270.
Line, M. B., Nordland, O., Røstad, L., & Tøndel, I. A. (2006). Safety vs. security? Paper presented at PSAM conference, New Orleans. Available here: https://www.researchgate.net/profile/Maria_Bartnes/publication/289479187_Line_etal_-_Safety_vs_Security_-_PSAM8_2006/links/568d02bc08aec2fdf6f50e92/Line-etal-Safety-vs-Security-PSAM8-2006.pdf
Liss, C. (2011). Oceans of crime: maritime piracy and transnational security in Southeast Asia and Bangladesh. Singapore: Institute of Southeast Asian Studies.
McNicholas, M. (2016). *Maritime security: An introduction*. Amsterdam: Elsevier.
Metaparti, P. (2010). Rhetoric, rationality and reality in post-9/11 maritime security. *Maritime Policy & Management: The Flagship Journal of International Shipping and Port Research, 37*(7), 723–736.
Sauser, B., Baldwin, C., Pourreza, S., Randall, W., & Nowicki, D. (2018). Resilience of small-and medium-sized enterprises as a correlation to community impact: An agent-based modeling approach. *Natural Hazards, 90*(1), 79–99.
Talley, W. (2013). *Maritime safety, security and piracy.* London: Informa.
Von Hoesslin, K. (2005) Maritime regulation & shipping: How is the ISPS Code affecting your business?. Available at: http://www.conflicts.rem33.com/images/terrorism/von_Hoesslin.htm

Further Reading

Oltedal, H. A., & Lützhöft, M. (2018). *Managing maritime safety.* New York: Routledge.
Talley, W. (2013). *Maritime safety, security and piracy.* London: Informa.

Mercenary and Private Military

Spyridon Triantafyllou
John Jay College of Criminal Justice, New York, NY, USA

Keywords
Private security · Contractors · Security services · Mercenaries · International law

Definition

Non-state security providers, companies offering private military and security services.

Introduction

Other similar or related terms: *Private Military Companies* (PMCs), *Private Security Companies* (PSCs), *Private Military Firms* (PMFs), or *Private Military and Security Companies* (PMSCs). For practical reasons, the adoption of generic term "PMSCs" is suggested, despite the controversy upon the distinction of these terms (Singer 2003).

According to the UN Draft Convention on Private Military and Security Contractors (2011), PMSCs offer security or military services, defining "security services as armed guarding of things or people, knowledge transfer with security/police applications, development and implementation of informational security measures and other related activities."

Private Security Companies (PSCs) – compared with Private Military Companies (PMCs) – are not involved directly with combat activities and operate under a greater mandate, offering not only military services, but also other security services on a strategic, tactical, and operational level, such as policing, advising, and logistical support. Alternatively, the distinction between military and security services derives from the nature of the services, in that

participating as a combatant or offering other services, respectively.

Private Military Firms (PMFs) term indicates the contemporary trend of privateering and outsourcing of security functions, which are inherently governmental functions as security is a public good.

The type and extent of private security services varies depending on the host nation and the contractor (company). There may be active and/or passive security measures in place, while focusing on police operations, several security services are offered including protection of assets or any other activity for which carrying or operating a weapon in performance is required. Finally, peacekeeping and other support mission services are offered related to security sector reform (reform of the police and the judiciary), including training and capacity-building activities.

Need for Private Security Services

According to the Montreux Document (2008), Private Military and Security Companies (PMSCs) are "private business entities that provide military and/or security services, irrespective of how they describe themselves. Military and security services include, in particular armed guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel." In addition, according to the International Code of Conduct (ICoC) (2010), private security services may be offered by unarmed personnel.

The scope of PMSCs activities is to protect assets (persons, properties, proprietary information, reputation) in countries where security is deficient or when conflicts or disasters necessitate increased security measures.

A recent motion for action of the European Parliament highlights the importance of PMSCs in support of operations abroad. Such private entities: "1. *(should)* play an important complementary role in aiding the state's military and civilian agencies by closing capability gaps created by increasing demand for the use of forces abroad, *(. . .)* 3. compared to national troops, can provide valuable local knowledge and, frequently, cost savings, although it must be ensured that quality is not undermined, *(. . .)* 4. no activities should be outsourced that would imply the use of force and/or active participation in hostilities, except for self-defence *(and)* any participation by private security companies in military operations must be justified, with clearly-defined objectives that can be verified using tangible indicators, have a fully-detailed budget and a specific start and end date, and be governed by a strict code of ethics *(. . .)*" (European Parliament 2017).

Clients of security services might be governments, international organizations (i.e., the United Nations, European Union), non-corporate security providers (i.e., host government military and police, local militias, peacekeeping forces), humanitarian organizations or NGOs, private industries to ensure their economic interests (i.e., oil, gas, mining, transportation sectors), or journalists. In such cases, usually there is no guarantee for protection due to weakened governance in terms of stability and development of the host nation.

Prior to signing a contract with PMSCs, potential clients should take into consideration if the company complies with the law and a code of ethics, particularly in: "a) acquiring information relating to the principal services the PMSC has provided in the past; b) obtaining references from clients for whom the PMSC has previously provided similar services to those the contracting state is seeking to acquire; c) acquiring information relating to the PMSC's ownership structure and conducting background checks on the PMSC and its superior personnel, taking into account relations with subcontractors, subsidiary corporations and ventures" (Montreux Document 2008).

Several initiatives have taken place to establish accountability and transparency mechanisms of PMSCs and their activities with respect to international human rights and humanitarian law, national law, or other terms of the contract. These initiatives highlight the procedures for the selection of and contracting with PMSCs, as well as the assessment of risks so as to determine what

security services are necessary and why, based on a cost-benefit analysis both for host nation and contractor.

In terms of accountability, three phases are to be taken into consideration when focusing on contractors and their distinct relationships with the hiring, host, and home states: (1) the *contracting phase* (scope of activities outsourced, screening history and vetting); (2) the *in-the-field phase* (monitoring mechanisms and other regulatory bodies); and (3) the *post-conduct phase* (civil liability and criminal culpability issues of private contractors and their personnel) (Huskey 2012).

Jobs Performed by Mercenaries

Private security firms hire private military specialists who play key role in armed conflicts assuming their expertise, their integrity, and their apolitical origin (Mandel 2001). This is not a new phenomenon, as mercenaries were hired and extensively utilized to establish security and promote private interests from the Medieval times to nineteenth century. Some examples are the *condottieri* in Italy during the Renaissance period, the Swiss mercenaries who fought for the French until 1793, *privateering* as a wartime practice against pirates, and the *mercantile companies* or forces for the British, Dutch, and other colonies (see Andreopoulos and Brandle 2012).

Indicative of the types of private security services are the findings of a survey conducted to depict the role of the private security industry in support of humanitarian organizations, operating in complex and hostile environments (i.e., countries or regions in Central Africa, Middle East, North Caucasus). According to a Humanitarian Policy Group report (2008), the importance of security services in humanitarian operations, by both international and local security providers, is presented as follows (arranged in descending order):

- Unarmed guards for facilities/residences/project sites
- Physical security for premises
- Security management consulting
- Security training for staff
- Risk assessment/threat analysis
- Information services
- Armed guards for facilities/residences/project sites
- Standby security
- Mobile escorts (armed)
- Unarmed bodyguards
- Critical incident/crisis management
- Hotlines
- Logistics
- Armed bodyguards
- Mobile escorts (unarmed)
- Unarmed third party security
- Armed third party security

Mercenaryism should be differentiated from Private Military and Security Companies (PMSCs), which are private legal entities employing a significant number of staff on a fixed-term basis and oftentimes higher salary.

According to Article 47 of Protocol I additional to the 1949 Geneva Conventions, applicable in international armed conflicts, a mercenary is "any person who: a) is specially recruited locally or abroad in order to fight in an armed conflict; b) does, in fact, take a direct part in the hostilities; c) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party; d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; e) is not a member of the armed forces of a Party to the conflict; and f) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces."

Although the motivation of the contracted is not always clear, PMSC employees act as mercenaries, if all these criteria meet cumulatively. In such cases, they are not considered as combatants, and, thus, they are not entitled to prisoner of war (PoW) status, according to the law of armed conflict.

Locations Used of Private Military and Security Companies

Private Security Companies as a whole appeared in the 1970s, but they were especially preferred and deployed during the "war on terror," particularly in Afghanistan and Iraq wars after 9/11 attacks and against the Islamist State of Iraq and the Levant (ISIL/ISIS) terror group, as well in other post-conflict areas or situations.

Either offering purely security services or other auxiliary services, there are several PMSCs, which operate in several areas worldwide. Usually, they support governments (host, hiring) or organizations to establish to national security, public order, or peace-building capacities in areas suffering from sociopolitical stability, civil wars, humanitarian crises, or lack of governance ("failed states").

Such examples include, but are not limited to, the United Nations perspective, which hired PMSCs to operate in high-risk environments especially during the first decade after the 2000s: provision of civilian personnel in UN missions in *Haiti and Liberia* (2004); peacekeeping and contingency operations in *African countries* (2003, 2009); armed or unarmed security personnel for the protection of UN officials in *Iraq* war; physical security and training in *Kenya* and *Afghanistan*; supply helicopter transport and satellite network in *East Timor* (2008); logistical and intelligence support in *Sierra Leone* (2000, 2003) or *Democratic Republic of Congo* (2001); logistics connected with security (i.e., information-gathering and intelligence-like services), such as provision of public security in *Iraqi* referendum (2005); monitor sanctions in *Angola* (2001); intelligence operations in *Iraq*, *Sudan*, and *Afghanistan*; removal of unexploded landmines in *Sudan* (2006) and of improvised explosion devices in *Nepal* (2007); clearance and training in *Bosnia* and *Mozambique* (2008); or demining of the buffer zone of *Cyprus* (see Østensen 2011).

Over the last decade and because of attempts to legally regulate private security sector operating abroad as discussed next, PMSCs have transformed their activities according to security sector reform initiatives or other procurement-oriented services into human rights training, capacity building of local military and police corps, and military to civil transition support.

Additional Issues and Concerns

On September 16, 2007, in Nisour Square (Baghdad, Iraq), a US embassy convoy escorted by security guards of "Blackwater Security Consulting" was attacked, who in turn fired back, resulting in 17 dead and 20 injured civilians. The shooting incident was the critical juncture; since then, mercenaries are in the public eye and more regulation of the field under the international humanitarian law was initiated to deal with unnecessary or disproportionate violence PMSC personnel.

Aiming to clarify the international legal framework regarding PMSCs and to benchmark good conduct of private security industry, initiatives run by Swiss Government and other actors led to the Montreux Document (2008) and finally to the International Code of Conduct (ICoC) (2010). According to the ICoC, the main *principles* refer to general conduct, use of force, detention, prohibition of torture, trafficking in human beings and sexual exploitation, discrimination, and identification and registering policies for PMSCs and their personnel, while the primary *commitments* refer to incorporation of code of conduct into company policies, selection and vetting of personnel and subcontractors, training, incident reporting, and liability issues regarding PMSCs.

Moreover, in 2010, a "Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council" was annexed in a Report of "UN Working Group on Use of Mercenaries as a Means of Violating and Impeding the Exercise of Rights of Peoples to Self-Determination." The UN has attempted to introduce restrictive and universal standards (including states and international organizations), applicable not only in armed conflicts, but in all certain situations involving private security contractors with respect to international humanitarian law.

All these legal, not-binding though, documents attempt to set out principles and standards for

PMSCs based on international law and accountability, but they commit only the signatory parties as there is a "soft law" approach for industry regulation.

Private security services constitute a significant challenge for an international system. On the one hand, security is public responsibility connected with national sovereignty. On the other hand, the non-statutory nature of contractors is attached with financial motivation and business practices and, therefore, impacts on the national response to regulation of private security. The main question under scrutiny is whether private entities can exert violence by supporting nations or other companies and in what manner. Therefore, apart from the legal framework, a code of conduct is essential to oversight private security contractors.

Conclusion

To conclude, it is widely accepted that the use of force by PMSCs should be restricted in to use in self-defense or defense of others (like civilians), which implies the nature of PMSCs. Consequently, private security contractors do not have more privileges or rights to use force than other civilians. Finally, nowadays, PMSCs support the mission of military or police, but they have a distinct role since the state agents have the monopoly of violence to ensure public safety, including powers of arrest, search, and seizure (Buzatu 2015).

Cross-References

▶ EU Private Security Regulation
▶ Security: Private

References

Buzatu, A.-M. (2015). Private military and security companies in CSDP missions. In *Handbook on CSDP missions and operations, The common security and defence policy of the European Union*. Vienna: Directorate for Security Policy of the Federal Ministry of Defence and Sports of the Republic of Austria.

European Parliament. (2017). Report on private security companies, *Committee on Foreign Affairs, Rapporteur: Hilde Vautmans*, Report 2016/2238 (INI).

Huskey, K. (2012). Accountability for private military and security contractors in the international legal regime. *Criminal Justice Ethics, 31*(3), 193–212.

Mandel, R. (2001). The privatization of security. *Armed Forces & Society, 28*(1), 129–151.

Singer, P. W. (2003). *Corporate warriors: The rise of privatized military industry*. Ithaca: Cornell University Press.

Stoddard, A., Harmer, A., & DiDomenico, V. (2008). *The use of private security providers and services in humanitarian operations* (Humanitarian Policy Group report 27). London: Overseas Development Institute.

The Geneva Convention of 1949 and its Additional Protocols (1949).

The International Code of Conduct (ICoC) for Private Security Service Providers (2010).

The Montreux Document, On pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict on the use of Private Military Security Companies (2008).

The UN Draft of a possible Convention on Private Military and Security Companies (PMSCs) for consideration and action by the Human Rights Council (A/HRC/WG.10/1/2) (2011).

Further Reading

Andreopoulos, G., & Brandle, S. (2012). Revisiting the role of private military and security companies. *Criminal Justice Ethics, 31*(3), 138–157.

Krahmann, E. (2010). *States, citizens and the privatization of security*. Cambridge: Cambridge University Press.

Østensen, A. (2011). *UN use of private military and security companies: Practices and policies* (SSR paper 3). Geneva: The Geneva Centre for the Democratic Control of Armed Forces (DCAF). https://www.dcaf.ch/sites/default/files/publications/documents/SSR_PAPER3.pdf

The UN Guidelines on the Use of Armed Security Services from Private Security Companies (2012).

N

Natural Hazards

Sara Bonati
SAGAS, Università degli studi di Firenze, Florence, Italy

Keywords
Hazards · Natural · Risk · Disaster

Definition

Natural hazards are geophysical processes that deviate from the norm by resulting in dangerous situations. They include sudden processes and slow long-term processes, such as expected and unexpected ones.

Introduction

Natural hazards are usually defined as the possibility that something dangerous may happen or that a risk can be manifested (Montz et al. 2017). According to Ball (1979), natural hazards are the manifestations of geophysical systems that deviate in a meaningful way from their long-term average. Similarly, Smith (1992) has defined natural hazards as extreme fluctuations or deviations of environmental processes. Other definitions consider the human dimension, such as dangerous scenarios that develop from the interaction between nature and human society (Burton et al. 1978).

The opposition between nature and society is not always enough to explain all the possible types of hazards, especially when the interaction is not clear or it does not fall into specific time-place limit (Khan 2012). This fusion between "natural" and "social" dimensions is increasing also in the approaches adopted to study hazards. Thus, it is frequent for studies of geophysical sciences to address social components of natural hazards (e.g., Jayasingha 2016), such as multi-disciplinary approaches to the topic (e.g., Frigerio et al. 2016). Today, natural hazards are broadly recognized as hazards that have natural, social, and socio-natural origins. Paron (2013) defines "hazards" as "highly anthropocentric in nature," being the result of an interaction between a biophysical process and an "occupying" group of people/community. Stewart (2013) elaborated that according to the science of natural disasters, hazards are causative events that nature shapes and produces, while the external negative consequences have to be investigated in the society.

In social sciences today, it is broadly accepted the idea that the concept of natural hazard is socially constructed, and therefore it is possible to talk effectively about them only if they are interpreted in relation to society. As Kelman (2018) stated, all hazards are "socially mediated." Kelman argued that when a natural process is mediated by society and its characteristics are modified in a way that makes it hazardous, it

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

is not possible to continue to talk about "natural" hazard. Thus, the distinction between natural hazard and human hazard is in some way sterile because it is quite complicated to distinguish among the various origins of the phenomenon and to identify the limits of social actions in transforming the environment. This assumption is also supported by Wisner et al. (2012) in that the natural environment is not considered entirely natural because it is subjected to human action: "Hazards are not entirely free of human influence, although some hazards are difficult to influence at a large scale such as space weather and earthquakes" (p. 24). The definition given by UNISDR (2017) recognized the potential role of humans in increasing the "hazardousness" of natural processes (also see Kelman 2018).

The human element in hazard interpretation prompts another question about the "unexpected" dimension of hazards. Usually, hazards are considered as something happening suddenly in an unexpected way; however, the role of humans in such hazards suggests that these hazards could be expected. Expectation does not mean that we are able to know the exact moment such hazards will occur, just that they will happen in time. For instance, some floods have origins in human intervention along rivers, fires can be a consequence of changing the bio-composition of forests, and even earthquakes can be produced by the human activity of hydraulic fracking.

Classification of Natural Hazards

There are multiple ways to classify natural hazards. One method is according to their "physical dimension" at the origin of the event. For example, according to Bokwa (2013), there are geological hazards, like earthquakes and landslides; meteorological hazards, like cyclones and hurricanes; hydrological hazards, like floods; oceanographic hazards, like sea level rise; hazards connected with vegetation; and extraterrestrial hazards. UNISDR (2017) classified biological hazards, environmental hazards (that can also be technological), geological or geophysical hazards, hydrometeorological hazards, and multi-hazards. Another classification is according to their time-space manifestation and magnitude. Hazards are natural transformations of the environment that happen at both the local and global levels and that can be sudden or slow in their manifestation. The low probability that these events become disasters is usually responsible for low attention to the potential risk they represent (Montz et al. 2017).

Distinguishing Between Danger and Hazard

Danger is the possibility that something happens to an individual and that produces damages. More specifically, danger is the possibility that an individual will be harmed and is focused on the physical damages that the person or persons can suffer in terms of health and life. In contrast, a hazard is a process that can produce dangerous situations from which an individual can be harmed or be in danger. The definition of hazard is more focused on the "probability" that something happens. For example, a place is defined as hazardous if there is a high probability that a particular dangerous phenomenon will take place.

Distinguishing Between Risk and Hazard

Similarly, risk and hazard are two concepts that are usually confused; thus, it is difficult to identify a common interpretation that defines them without further discussion. This problem is increased by the fact that not all the languages can have direct translations of the concepts (this is the case, e.g., of Italian, where there is not a correspondence for "hazard" word; and this can become more complicated with languages that adopt a different alphabetical system).

In disaster studies, risk is usually considered the first path to disaster; it is the condition without which a disaster cannot take shape. Risk requires two conditions: an element that produces the risk and the possibility of damages (i.e., danger,

exposure, vulnerability). In contrast, hazards represent those phenomena that can "expose" a person to vulnerable situations (Kelman 2016). Another difference in these two terms is in a research approach; the risk approach focuses mainly on the damages, while the hazard approach focuses on the processes that can produce those damages.

Distinguishing Between Natural Hazards and Unnatural Disasters

According to a World Bank report (UN 2010), "the adjective 'UnNatural' in the title of this report conveys its key message: earthquakes, droughts, floods, and storms are natural hazards, but the unnatural disasters are deaths and damages that result from human acts of omission and commission" (p. 1). Not all earthquakes become disasters. If a society has the capacity to deal with a particular event and this takes place without the production of damages, that is a hazard but not a disaster. As Quarantelli wrote: "A disaster is not a physical happening. It is a social occasion" (2005, p. 343; see also Squires and Hartman 2013). Disasters and hazards are distinguished by the social dimension that Birkmann (2006) and Blaikie et al. (2004) define as vulnerability (see also Wisner et al. 2012).

In disaster studies, hazard and disaster are distinguished by the point of view adopted. Accordingly, Gaillard and Mercer (2013) identify two paradigms in disaster studies: hazard paradigm and vulnerability paradigm. The hazard paradigm is focused on the dynamics of the physical happening. *Hazard* is a "judgment" of a normal (and sometimes essential) natural process that comes from choices adopted from societies over the long term, choices that are responsible for the dangerous dimension of events (Kelman 2009). This paradigm is founded on works by Burton et al. (1978) and Kates (1971) who say that disasters come from the inability of people to "adjust" to avoid damages. Natural hazards can be also read as resilient processes put in place by nature to adapt to and answer to human transformations. The focus is on the ability to deal with and understand the level of risk to which people are exposed. On the other side, the vulnerability paradigm is oriented to discuss the social dimension of the event in terms of damages and exposure. It focuses on the level of vulnerability of the people exposed and on the processes that were brought to this. In particular, processes of marginalization and lack of rights are considered, according to political ecology and environmental justice (e.g., Bolin and Kurtz 2018; Cutter 2012; Wisner et al. 2004).

Conclusion

Natural hazards are slow and fast processes that can produce damages and that can become disasters if some risks take shape. The hazard research approach is focused mainly on the "nature" of the process and its dynamics and on the following human adjustments. Not all hazards become disasters; it depends by the presence of vulnerability conditions. In literature the expression "natural hazard" is accepted and used, and it refers to different physical processes, although some authors discuss the "natural dimension" of some hazards. To conclude, hazards, risks, and disasters have not to be confused, and the dimension of vulnerability is at the basis of their distinction.

Cross-References

- ▶ Natural Hazards
- ▶ Natural Hazards: Earthquakes
- ▶ Natural Hazards: Floods
- ▶ Natural Hazards: Hurricanes, Cyclones, and Typhoons
- ▶ Natural Hazards: Pandemic Threats by Infectious Diseases
- ▶ Natural Hazards: Tornadoes
- ▶ Natural Hazards: Tsunamis
- ▶ Natural Hazards: Volcanic Eruptions
- ▶ Risk Analysis: National and International Standards

References

Ball, N. (1979). Some notes on defining disaster: Suggestions for a disaster continuum. *Disasters, 3*(1), 3–7.

Birkmann, J. (2006). Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions. In *Measuring vulnerability to natural hazards: Towards disaster resilient societies* (Vol. 1, pp. 9–54). United Nations University Press.

Blaikie, P., Cannon, T., Davis, I., & Wisner, B. (2004). *At risk: Natural hazards, people's vulnerability and disasters*. New York: Routledge.

Bokwa, A. (2013). Natural hazard. In *Encyclopedia of natural hazards* (pp. 711–718). Dordrecht: Springer.

Bolin, B., & Kurtz, L. C. (2018). Race, class, ethnicity, and disaster vulnerability. In *Handbook of disaster research* (pp. 181–203). Cham: Springer.

Burton, I., Kates, R. W., & White, G. (1978). *The environment as hazard*. New York: Oxford University Press.

Cutter, S. L. (2012). *Hazards vulnerability and environmental justice*. New York: Routledge.

Frigerio, I., Ventura, S., Strigaro, D., Mattavelli, M., De Amicis, M., Mugnano, S., & Boffi, M. (2016). A GIS-based approach to identify the spatial variability of social vulnerability to seismic hazard in Italy. *Applied Geography, 74*, 12–22.

Gaillard, J. C., & Mercer, J. (2013). From knowledge to action: Bridging gaps in disaster risk reduction. *Progress in Human Geography, 37*(1), 93–114.

Jayasingha, P. (2016). Social geology and landslide disaster risk reduction in Sri Lanka. *Journal of Tropical Forestry and Environment, 6*(2), 1–13. http://journals.sjp.ac.lk/index.php/JTFE/article/view/2938/1979

Kates, R. W. (1971). Natural hazard in human ecological perspective: Hypotheses and models. *Economic Geography, 47*(3), 438–451.

Kelman, I. (2009). Understanding Vulnerability to Understand Disasters. Version 3, 19 January 2009 (Version 1 was 2 September 2007). Available at: www.islandvulnerability.org/docs/vulnres.pdf.

Kelman, I. (2016). Environmental hazards. In *International encyclopedia of geography: People, the earth, environment and technology* (pp. 1–19). Wiley

Kelman, I. (2018). Lost for words amongst disaster risk science vocabulary? *International Journal of Disaster Risk Science, 9*(3), 281–291.

Khan, S. (2012). Disasters: Contributions of hazardscape and gaps in response practices. *Natural Hazards and Earth System Sciences, 12*(12), 3775–3787.

Montz, B. E., Tobin, G. A., & Hagelman, R. R. (2017). *Natural hazards: Explanation and integration*. New York: Guilford Publications.

Paron, P. (2013). Natural hazards in developing countries. In P. T. Bobrowsky (Ed.), *Encyclopedia of natural hazards. Encyclopedia of earth sciences series*. Dordrecht: Springer.

Quarantelli, E. L. (2005). A social Science Research Agenda for the 21st century: Theoretical, Methodological and Empirical Issues and their Professional Implementation. In: Ronald Perry and E. L. Quarantelli (Eds.), What is a disaster? New answers to old questions (pp. 325–396). Xlibris.

Smith, K. (1992). Environmental hazards: Assessing risk and reducing disaster. *Environment International, 3*(23), 422.

Squires, G., & Hartman, C. (2013). *There is no such thing as a natural disaster: Race, class, and Hurricane Katrina*. New York: Routledge.

Stewart, I. (2013). Disasters. In P. T. Bobrowsky (Ed.), *Encyclopedia of natural hazards. Encyclopedia of earth sciences series*. Dordrecht: Springer.

UNISDR (United Nations Office for Disaster Risk Reduction). (2017). *Terminology on disaster risk reduction*. Geneva: UNISDR. https://www.unisdr.org/we/inform/terminology. Accessed 11 Nov 2018.

United Nations. (2010). *Natural hazards, unnatural disasters: The economics of effective prevention*. Washington, D.C.: The World Bank.

Wisner, B., Blaikie, P. M., Blaikie, P., Cannon, T., Davis, I. (2004). At risk: natural hazards, people's vulnerability and disasters. Psychology Press.

Wisner, B., Gaillard, J. C., & Kelman, I. (Eds.). (2012). *Handbook of hazards and disaster risk reduction and management*. London: Routledge.

Further Reading

Gaillard, J. C. (2016). Natural hazards and disasters. In *International encyclopedia of geography: People, the earth, environment and technology: people, the earth, environment and technology* (pp. 1–15). Wiley.

Gaillard, J. C., Cadag, J. R. D., & Rampengan, M. M. (2018). People's capacities in facing hazards and disasters: An overview. *Natural Hazards, 95*(3), 863–876.

Natural Hazards: Earthquakes

Hua-Lun Huang
Department of Sociology, Anthropology, and Child and Family Studies, University of Louisiana, Lafayette, LA, USA

Keywords

Major Earthqake · Secondary Earthquake · Geographic Location · Extraordinary Event · Ordinary Event

Definition

An earthquake is the shaking of the surface of the Earth. It is a force that can cause great damages to

man-made structures, such as airports, amusement facilities, bridges, commercial buildings, dams, government buildings, harbors, historical constructions, hospitals, libraries, military bases, museums, nuclear power plants, public statues, religious buildings, residential houses, roads, and schools. It can trigger massive landslides, mudslides, and tsunami as well.

Introduction

Earthquakes are a scary thing for numerous people, especially for those who live in areas rarely or never stricken by seismic activity. The reason for this collective fear is obvious:

The occurrence of earthquakes, at least in the early 2020s, remains unpredictable. As a result of this unpredictability (or capriciousness), no one can be certain that his/her property will never be damaged or destroyed by earthquakes (especially major ones) in the future.

While earthquakes can bring great damages to buildings and infrastructures, most of them tend to be moderate or insignificant. With this in mind, classifying earthquakes is a crucial job for those researchers who want to compare the social impacts brought about by earthquakes.

In terms of classifying earthquakes, seismologists and other investigators undoubtedly have many factors they can focus on, such as power (P), time (T), scope (S), or duration (D). Besides PTSD, seismologists can also concentrate on pattern when categorizing earthquakes.

For the purpose of comparison, seismic activities are classified into *MIE*, *MIO*, *MNE*, *MNO*, *SIE*, *SIO*, *SNE*, and *SNO* types in this entry. To explain this classification, this entry will aim to address the following two "big questions":

First, how to classify earthquakes from the angle of sociology?

Second, what are the defining characteristics of major and secondary earthquakes?

Technical issues related to earthquakes, however, will not be discussed for they are beyond the scope of this entry. These issues include, but are not limited to, the subsequent questions:

First, what are the most important technologies (i.e., earthquake warning technologies) that can help seismologists predict the happening of earthquakes?

Second, what are the devices that can help residents (especially those who live in regions frequently stricken by earthquakes) reduce the impacts of earthquakes?

Third, what are the best architectural designs that can prevent buildings (especially tall ones) from collapsing when major earthquakes take place?

Finally, what are the techniques that can help architects deal with the problems caused by earthquakes (e.g., liquefaction, sinkhole, landslide, etc.)?

A Sociological Classification of Earthquakes

In criminology and sociology, earthquakes are usually defined as a geological or geographical phenomenon. Because of this designation, the great majority of criminologists and sociologists did not attempt to classify earthquakes – after all, seismologists have already proposed several classification systems in the twentieth century (e.g., the Richter magnitude scale). As a result, advancing another categorization for earthquakes seems unnecessary.

Proposing another classification system for earthquakes, however, is by no means redundant – from the perspective of security (or emergency management), the taxonomies proposed by Charles Richter and other seismologists did not clearly and directly mention the social problems caused by earthquakes. Accordingly, the Richter magnitude scale and other similar measurements tend to be inadequate/insufficient in helping social scientists examine the relation between earthquakes and social actions (particularly criminal and deviant behaviors).

Based on the statements above, this entry will construct a classification system for earthquakes (which tend to concentrate in certain regions on earth, such as those countries located near or on the Ring of Fire). Three variables will be used to

create this system. They are intensity, geographic location, and social impact.

The Construction of a Classification System for Earthquakes

In sociology, one of the most significant approaches in explaining the emergence of a macro phenomenon (e.g., the formation of an extremist social movement) is structuralism. According to this approach, the appearance of a macro phenomenon always involves the interaction of two sets of variables. The first set is composed of structural factors, such as ecological resource, government pattern, religious institution, population density, and technological level. According to Giddens' (1986: 25–34) theory of structuration, these factors can help a society maintain stability or demonstrate stable features. They can be characterized as "temporal continuity" (Little 1991:103) because they will last for years and serve as boundaries constraining the actions of social members.

The second set of variables is composed of actors/agents who can establish various relationships (Roth and Wittich 1978: 38–46). Unlike structural factors that can help a society preserve miscellaneous laws/rules and maintain "administrative and regulative" order (Roth and Wittich 1978: 51), the actions taken by agents may trigger changes in a society. Agents are therefore the sources of progression/transformation and the producers of temporal variation.

Inspired by the three concepts of structure, agency, and interaction (i.e., the interplay between structure and agency), earthquakes are grouped by three-level variables in this entry. The first variable, *intensity*, stems from the concept of structure. It refers to the magnitude or geographical reach of an earthquake. The second variable, *geographic location*, comes from the notion of agency. It represents the variations of earthquakes in space or physical position. The third variable, *impact*, derives from the idea of interaction. It denotes the damages (which can be visible/serious or invisible/minor) that an earthquake causes in a certain area. Each of the three variables is divided into two levels:

First, *intensity* is split into major (M) [which are those seismic activities that reach 7.0 or higher in the Richter magnitude scale] or secondary (S) [which are those seismic activities that do not exceed 6.9 in the Richter magnitude scale].

Second, *geographic location* is divided into involved (I) [which are those earthquakes that can directly send seismic waves to populated areas because the epicenter is close to or on the verge of human settlements] or uninvolved (U) [which are those earthquakes that do not directly send seismic waves to any populated areas because the epicenter is far away from human settlements].

Finally, *impact* is divided into extraordinary (E) [which are those seismic activities classified by historians or seismologists as textbook examples or landmark events] or ordinary (O) [which are those seismic activities not regarded by historians or seismologists as model or milestone instances].

Based on the different combinations of the above-listed ranked variables, a classification system for earthquakes can be seen in the following:

- The *MIE* type (i.e., *major* earthquake + *involved* + *extraordinary event*).
- The *MIO* type (i.e., *major* earthquake + *involved* + *ordinary* event).
- The *MUE* type (i.e., *major* earthquake + *uninvolved* + *extraordinary event*).
- The *MUO* type (i.e., *major* earthquake + *uninvolved* + *ordinary* event).
- The *SIE* type (i.e., *secondary* earthquake + *involved* + *extraordinary event*).
- The *SIO* type (i.e., *secondary* earthquake + *involved* + *ordinary* event).
- The *SUE* type (i.e., *secondary* earthquake + *uninvolved* + *extraordinary event*).
- The *SUO* type (i.e., *secondary* earthquake + *uninvolved* + *ordinary* event).

The classification scheme advanced in this entry therefore includes eight categories of earthquakes. Since each typology has certain implications in security and emergency management, they will be summarized in the section of Conclusion. Before inspecting the possible

consequences brought about by seismic activities, the defining characteristics of major and secondary earthquakes will be first addressed. These core features will be exemplified by earthquakes that took place in Central Asia, East Asia, North America, and the South Pacific in the twentieth and twenty-first centuries.

The Defining Characteristics of Major and Secondary Earthquakes

As stated, earthquakes (no matter whether they are contemporary or ancient cases) can be characterized as *MIE*, *MIO*, *MNE*, *MNO*, *SIE*, *SIO*, *SNE*, or *SNO* type. That means some earthquakes are fairly similar, some are partially similar, some are considerably dissimilar, while others are totally different.

Given that seismic activities are diverse in power, epicenter, or aftermath, comparing the central qualities of major and secondary earthquakes is therefore an essential component in helping crime researchers identify those circumstances under which seismic activities can become criminogenic (i.e., identify those opportunity structures that can provide people with chances to commit crime or launch extremist movements).

In the following, the central features of major earthquakes will be first inspected and contrasted. Then the main traits of secondary earthquakes will be examined and compared.

MIE-Type Earthquake

According to reports/measurements, some earthquakes that took place on earth in the past decade reached 7.0 or higher in the Richter magnitude scale – some were somewhere between 7.0 and 8.9, while a small number of them were above 9.0. No matter whether an earthquake attained the highest level in the Richter magnitude scale (i.e., the range of 9.0 to 10.0), seismic activities (if they are close to a city) can always severely damage buildings and infrastructures if they reach at least 7.0 or higher in the Richter magnitude scale. For this very reason, all seismic activities that arrive at 7.0 or higher in the Richter magnitude scale can be classified as major earthquakes.

Major earthquakes, on the other hand, do not concentrate in particular areas only – according to records, some took place in regions far from cities (e.g., deep ocean, desert, isolated island, etc), some happened in districts not too close or too far from cities, while others occurred on the verge of densely populated cities. In this regard, the *MIE*-type earthquakes can always bring great damages to a city because the location of these shakings is very close to a populous area, which allows the *MIE*-type quakes to deeply get involved in the routine life of human societies.

So the *MIE*-type earthquakes are by no means trivial or negligible events. On the contrary, they are extraordinary incidents for they can cause extensive damages in stricken cities. This devastating effect can be plainly seen in the Japan earthquake of 2011, the Haiti earthquake of 2010, the Sichuan (China) earthquake of 2008, the Taiwan earthquake of 1999, the Tangshan (China) earthquake of 1976, the Alaska earthquake of 1964, the Chile earthquake of 1960, and the San Francisco earthquake of 1906 (see Freedman 2013; Miles 2017; Palmer 2012; Svistova and Pyles 2018; Takezawa 2016; Yong and Booth 2011).

Although the *MIE*-type earthquakes can lead to great casualties when they take place, accurately predicting the occurrence of this kind of earthquakes (at least so far) is not likely. For this reason, the *MIE*-type earthquakes can always turn a stricken region into a hotspot of crimes if people of that area fail to fix damaged or derelict buildings as soon as possible (for these structures can become shelter for delinquent and marginalized populations).

MIO-Type Earthquake

Like the *MIE*-type earthquakes, the *MIO*-type quakes are powerful and potentially destructive. However, the *MIO*-type earthquakes do not occur in regions where seismic waves can directly and effectively affect metropolitan areas (or megacities). Instead, these quakes take place in sparsely populated places, such as countryside, peripheral rural towns, and gemeinschaft communities. That makes the *MIO*-type earthquakes look like a matter of little consequence.

While the *MIO*-type quakes rarely draw attention of the public because they do not happen in densely populated districts and will not bring massive damages, this does not imply that these earthquakes are totally noninfluential or negligible. Instead, the *MIO*-type quakes, just like the *MIE*-type quakes, are noteworthy because they allow the public to witness the destructive power of a major earthquake – in other words, the *MIO*-type quakes still can help seismologists or the public collect data about major shakings, even though these quakes usually strike tiny communities or small rural towns.

No matter how many *MIO*-type quakes will take place in the future, the media normally will not report these seismic movements in detail for they are not dramatic or spectacular enough in capturing the attention of the public. With this in mind, classifying these earthquakes as common events seems adequate.

Of the numerous earthquakes that have happened in the past two decades, the Altai earthquake of 2003 appears to be the best example of the *MIO*-type quakes. First, the intensity of this earthquake was higher than 7.0 in the Richter magnitude. Second, it did strike some rural communities. Nevertheless, the Altai earthquake was not considered to be spectacular because the casualties it caused were much lighter than those brought about by the *MIE*-type quakes.

In brief, the Altai quake did not have an extremely high death toll. For this very reason, finding academic books or reports on this quake is therefore extremely difficult, if not impossible. Wikipedia (see the article entitled *2003 Altai earthquake*) probably is the only source that can help the public obtain critical information on this earthquake.

MUE-Type Earthquake

Compared to the *MIE*- and the *MIO*-type earthquakes, the *MUE*-type quakes are far less common. The reason for this is that finding earthquakes (especially modern ones) that simultaneously exhibited the following three qualities is extremely difficult, if not impossible:

First, they are powerful (i.e., they reached 7.0 or higher in the Richter magnitude scale). Second, they do not send seismic waves to human settlements. Third, they are landmark events for humans, even though they do not have direct impacts on human communities.

Based on the three criteria listed above, it seems adequate to argue that the *MUE*-type quakes concentrated in prehistoric times:

Before humans started to establish settlements in the middle (and/or final) period of the Stone Age, certain strong quakes did take place on earth. Since some of these earthquakes were so powerful that mountain building and/or continental drift processes were triggered (see Frisch et al. 2011; Fountain 2017), such quakes did constitute milestone events for humans (although they happened in periods when structured settlements created by humans had not had taken shape), put differently, the mega-earthquakes that occurred in the Stone Age or earlier shaped the layout of continents and islands on earth. As a result of this geographic arrangement, numerous activities that humans engaged in were constrained by geographic characteristics. For example, modern-day Chinese peasants are far more likely to engage in small-scale farming than their American counterparts because China lacks areas that resemble the Great Plains of North America.

In brief, the *MUE*-type quakes are critical events for humans as they created the geographical spaces of the modern world, such as continents, gorges, islands, mountains, plateaus, peninsulas, and valleys. Such spaces, in turn, serve as physical boundaries of human activities. This may explain why humans always face particular environmental limitations after they have permanently dwelled in a certain region. For example, most parts of America do not produce rare earth-like scandium, yttrium, and neodymium. Because of this constraint, America must import rare earth from overseas, especially China, on a routine basis.

MUO-Type Earthquake

Unlike earthquakes of the *MIE* and *MUE* categories, the *MUO*-type quakes tend to play a trivial, if not totally inconsequential, role in human history. This "minor status" seems to be related to the following reasons:

First, the *MUO*-type quakes usually take place at the bottom of the ocean. Accordingly, these earthquakes normally will not affect human settlements, particularly large urban areas. Given that the *MUO*-type quakes, on average, do not seem to affect any human communities, the public naturally will not pay close attention to these seismic activities. This strongly implies that the *MUO*-type quakes are very likely to be forgotten by the public if they are not recorded by seismologists or other researchers.

One representative example of the *MUO*-type quakes is the underwater shaking that took place in the sea area near Taiwan's Hengchun peninsula in December, 2006 – even though this quake reached 7.1 in the Richter magnitude scale, it did not cause any damages in Taiwan and the Philippines. Seismologists therefore view this event as just a regular energy release from the inside of the earth (see the article entitled *2006 Hengchun earthquakes* in Wikipedia).

SIE-Type Earthquake

While several major earthquakes have struck both densely and sparsely populated areas on earth in the past 20 years, such quakes appear rare in human history. In other words, the great majority of earthquakes that happened in the modern world tend to be secondary because these seismic activities can be found in many places on earth almost every week.

Although most quakes that took place in the twentieth and twenty-first centuries look minor or insignificant, this does not imply that all of them are inconsequential. As a matter of fact, some secondary quakes are noteworthy because they can bring "hidden damages" to buildings, bridges, and roads, especially those made out of shoddy materials:

Like major earthquakes, secondary quakes can undermine the infrastructures of a city/metropolitan area as well. Such harms, however, seem much lighter than those caused by major earthquakes because secondary quakes usually are not powerful enough in bringing serious or immediately identifiable damages to a building or facility – this may explain why the destruction brought about by secondary quakes can remain undetected or unnoticed for a period of time. Under such circumstance, a seemingly normal building or facility may suddenly collapse or disintegrate if this structure experienced the above-noted "hidden damages" several times.

One probable case of the *SIE*-type quakes is the Hualien earthquake:

In February 2018, Hualien, the largest city of eastern Taiwan, was stricken by an earthquake. This quake, if it had had not caused high casualties and widespread injuries, is not shocking at all for its intensity merely reached 6.4 in the Richter magnitude scale. The Hualien earthquake, however, was not an ordinary shaking – not only did it partially or critically damage many buildings in Hualien, it also killed or wounded more than 300 people. All of these losses and casualties motivated Japan and Singapore to send rescue team or relief supplies to Taiwan (see the article entitled *2018 Hualien earthquake* in Wikipedia).

No matter whether Hualien will experience another earthquake in the near future, the high casualties caused by the 2018 earthquake in Hualien seemed to be closely related to the accumulative effect of "hidden damages." That is, Hualien, like those cities located on the Ring of Fire, has experienced numerous secondary earthquakes in the twenty-first century. Since these shakings might have led to structural deteriorations, which might remain invisible or look inconsequential for a long period of time, in the past 20 years, such structural declines or deformations (which probably had reached the critical point of disorganization or breakdown in 2018) helped the 2018 earthquake become a devastating one.

SIO-Type Earthquake

In terms of frequency and severity, most earthquakes that struck small towns or metropolitan areas in the twenty-first century tended to be weak. For example, California was stricken by several earthquakes in the nineteenth, twentieth, and twenty-first centuries; most of them, however, did not exceed 7.0 in the Richter magnitude scale (see the article entitled *List of earthquakes in California* in Wikipedia). For this reason, the *SIO*-type earthquakes are the most common pattern of shakings in the modern world.

Although the *SIO*-type quakes frequently occur and may look harmless, they are by no means risk-free. On the contrary, they can lay a long-term or irreversible foundation for the emergence of the *SIE*-type quakes (see the Hualien earthquake above).

Since the *SIO*-type earthquakes are enormous in quantity and similar in intensity, finding a "typical" or "outstanding" example for this category of seismic activities is extremely difficult and therefore impractical.

SUE-Type Earthquake

In comparison with the six categories of earthquakes examined in the previous pages, the *SUE*-type quakes might look "far less threatening" because of the following factors:

First, compared to the major earthquakes addressed in the previous pages, the *SUE*-type quakes are significantly weaker because they do not surpass 7.0 in the Richter magnitude scale. In addition to low intensity, the *SUE*-type quakes do not strike human communities. Instead, these secondary quakes concentrate in unpopulated regions like deserts, tiny volcanic islands, high mountains, or wastelands.

While the *SUE*-type quakes may look "less dangerous" than major earthquakes as well as the *SIE*- and the *SIO*-type shakings, they are still seismic activities of some importance. That is, the *SUE*-type quakes can become critical events if they trigger catastrophic outcomes – in other words, the *SUE*-type quakes play the role of "catalytic agents" (or initiator) in terms of "waking up" a major earthquake. Because of this role, the *SUE*-type quakes can induce a major earthquake to strike a city. The latter, in turn, can bring severe and extensive damages to a city, particularly infrastructure breakdown.

The *SUE*-type quakes can be caused by natural factors (e.g., volcanic eruption) or artificial reasons (e.g., nuclear test). Regardless of this, the chain relationship between the *SUE*-type quakes and major earthquakes appears to remain unclear. Before this relationship is fully clarified by seismologists, finding an illustrative case for the *SUE*-type quakes seems unlikely.

SUO-Type Earthquake

The final category of seismic activities examined in this entry is the *SUO*-type quakes. Such earthquakes are very unlikely to attract the attention of the public because first, they do not exceed 7.0 in the Richter magnitude scale; second, they do not directly strike human settlements; and third, they do not bring any noteworthy or observable damages to a town or city.

Given that the *SUO*-type quakes are not strong in intensity and do not seem to influence any town or city, they are probably least threatening among all types of earthquakes. What should be noted is that even though the *SUO*-type quakes might be considered minor events, they may possibly evolve into the *SUE*-type quakes under certain situations. No matter whether this assumption is correct, more studies on seismic activities are, of course, needed.

Conclusion

In this entry, earthquakes are classified into eight typologies according to sociological perspective. Of these varying types, the *MIE* type is most likely to become a "criminogenic earthquake" because these seismic activities can bring tremendous damages to a large city. Such damages, in turn, can significantly weaken social control and produce social problems, such as the authorities having to take care of tens or even hundreds of thousands of people who suddenly become displaced persons. So unless those dilapidated buildings and facilities stricken by the *MIE*-type quakes (especially abandoned and evacuated ones) are swiftly repaired, these unoccupied structures usually will become ideal places for delinquent populations (or homeless persons) to engage in drug trade and other illegal activities. The same anomic (or disorganized) situation might, to a lesser extent, appear in those regions stricken by the *SIE*-type quakes.

In contrast, the *SUO*-type quakes are least likely to help hotspots of crime take shape because these secondary (or weak) seismic activities do not seem to have anything to do with human settlements.

Cross-References

- ▶ Natural Hazards: Tsunamis
- ▶ Natural Hazards: Volcanic Eruptions

References

Fountain, H. (2017). *The great quake: How the biggest earthquake in North America changed our understanding of the planet*. New York: Broadway Books.

Freedman, L. (2013). *Bad Friday: The great and terrible 1964Alaska earthquake*. Kenmore: Epicenter Press.

Frisch, W., Meschede, M., & Blakey, R. (2011). *Plate tectonics: Continental drift and mountain building*. New York: Springer.

Giddens, A. (1986). *The Constitution of society: Outline of the theory of structuration*. Berkeley/Los Angeles: University of California Press.

Little, D. (1991). *Varieties of social explanation: An introduction to the philosophy of social science*. Boulder: Westview Press.

Miles, K. (2017). *Quakeland: On the road to America's next devastating earthquake*. New York: Dutton.

Palmer, J. (2012). *Heaven cracks, earth shakes: The Tangshan earthquake and the death of Mao's China*. New York: Basic Books.

Roth, G., & Wittich, C. (Eds.). (1978). *Max weber: Economy and society – an outline of interpretive sociology*. Berkeley/Los Angeles: University of California Press.

Svistova, J., & Pyles, L. (2018). *Production of disaster and recovery in post-earthquake Haiti: Disaster industrial complex*. New York: Routledge.

Takezawa, S. (2016). *The aftermath of the 2011 East Japan earthquake and tsunami: Living among the rubble*. Lanham: Lexington Books.

Yong, C., & Booth, D. C. (2011). *The Wenchuan earthquake of 2008: Anatomy of a disaster*. New York: Springer.

Further Reading

Stein, S., & Wysessioin, M. (2002). *An introduction to seismology, earthquakes and earth structure*. Malden: Wiley-Blackwell.

Natural Hazards: Floods

Sara Bonati
SAGAS, Università degli studi di Firenze, Florence, Italy

Keywords

Hazards · Floods · Climate change · Justice

Definition

Floods refer to rising or overflowing of water from its normal course that temporarily or permanently inundates an area that is usually dry (White 1945).

Introduction

Floods are the first kind of hazard studied in the field of disaster social sciences. White (1945) was the first to shift the scientific focus from the physical dimension of floods to the social dimension in terms of response capacity. According to Tobin and Montz (2011), a social approach to hazard studies is needed because the geophysical sciences are unable to understand the level of exposure of the people who are at risk; therefore, consideration of the social dimension of a disaster is lacking. White (1945) is credited with the disaster approach (see ▶ "Natural Hazards") that tries to define central concepts, such as disasters, risks, vulnerability, and resilience. His work challenged the idea that hazard studies are the most competent of the scientific disciplines. The geophysical focus on a specific hazard fails to investigate the multiple interactions between different processes and scales that are at the basis of the disaster (Alexander 1997; Hewitt 2014). Today, a rich body of literature focuses on social vulnerability as a key concept to discuss the root origins of floods and on the methodologies to measure it adopting a place-based approach (Box et al. 2016; Karagiorgos et al. 2016; Kuhlicke et al. 2011; Mavhura et al. 2017; Nasiri et al. 2016; Koks et al. 2015; Oulahen et al. 2015; Rufat et al. 2015; Sayers et al. 2018).

Floods are a natural component of the hydrological cycle with the potential to cause fatalities, displacement, and damage to environment and economic development (EU Floods Directive, 2007/60/EC). Today, floods are one of the most concerning natural hazards in the world; thousands of people are exposed to floods, frequently resulting in deaths and considerable economic damages (Pesaresi et al. 2017; Johnson et al. 2007). Floods have been defined in different

ways, based on different characteristics. Substantially, floods are defined as temporary inundations of areas that are usually dry. Typically, floods are caused by "(1) the overflow of inland or tidal waters; (2) the unusual and rapid accumulation or runoff of surface waters from any source; and (3) mudslides (i.e., mudflows)" (Federal Emergency Management Agency/FEMA 2018) as a consequence of flooding and are characterized by the moving of mud or earth by the water. As discussed below, climate change is contributing to the phenomenon; however, the human dimension continues to be central to its development.

Accordingly, in the next section, both physical and human factors that contribute to defining floods are discussed. In particular, there is an attempt to classify floods according to physical characteristics and a brief discussion on how climate change can affect floods' frequency and features. Then, the discussion is focused on the human dimension of floods and, in particular, on social behavior and social justice implications of such events.

Classifying Floods

There is no universal taxonomy on floods. Thus, different classifications are suggested in the literature. According to Johnson et al. (2007), floods can be defined based on their magnitude and occurrence. Several measures are used to quantify floods, including peak streamflow, rate of flow, water level increases, flow velocity, area or duration of inundation, frequency (Fischer and Schumann 2018), and severity (Kundzewicz et al. 2013; see also Kvočka et al. 2016). Other factors that influence floods are location, rain patterns, and basin catchment characteristics. A second way to classify floods is according to their main geographical characteristic, such as coastal floods and fluvial floods. Coastal floods, also known less frequently as sea floods, can be the consequence of high tides, storm surges, strong winds, and increases in sea levels. Fluvial floods, also known as riverine floods, are usually due to rainfall and snowmelt (Johnson et al. 2007; Blöschl et al. 2017). Johnson et al. (2007) referred to a third way of classifying floods, according to the time/space relationship. Accordingly, Rufat et al. (2015) noted that floods can be rare or frequent events with a long duration or a short duration. For example, flash floods, which suddenly occur in a specific area, can happen everywhere. According to the International Federation of Red Cross and Red Crescent Societies (IFRC), flash floods cannot be forecasted because of their rapid onset. Moreover, these hazards give people a very short amount of time to escape. In contrast, widespread floods follow a long period of rains or other weather phenomena, such as cyclones.

According to the Federal Emergency Management Agency (FEMA 2018) classification, shallow flooding and alluvial fan flooding are two other ways to classify flooding. The former type refers to floodings that do not exceed 3.0 ft of depth and where there are no water channeling systems; it is alluvial plains, depressions zones where they can form ponding areas, overbank and overland flows. The latter type is characterized by a high-velocity torrent flooding carrying water, rocks, mud, and debris and is typical in mountainous regions. This hazard is usually a consequence of high-intensity and short-duration rainfalls. The main physical consequences of alluvial fan flooding are erosion and sediment deposition. Recent forest fires, scarcity of vegetation, and other activities that make the slope soils unstable can have consequences on the characteristics of alluvial fan flooding. When the concentration of sediment in the flow corresponds to 20–40% of the volume, the hazard is considered a mud flow. Mud flows can have devastating effects in urban contexts, considering the velocity and their destructive potential (FEMA 2018).

Climate Change Effects on Flooding

In the last 30 years, episodes of extreme floods have occurred with more frequency and magnitude (Berghuijs et al. 2017). If it is difficult to identify the real weight that climate change has had in this change, it is expected that it

will have consequences on the future trends. According to the Intergovernmental Panel on Climate Change (IPCC) reports (2014, 2018), floods will undergo variations as a result of climate change. The predicted changes in temperatures and precipitation (e.g., Lee et al. 2018) as well as the early melting of snow and the anticipated peaks in rivers generated by glaciers melting should produce effects on frequency and magnitude of floods.

The extreme increase in the sea levels is a second relevant point to consider in relation to climate change and floods. According to IPCC report 2014, on a global scale, the trends of extreme episodes of high coastal water reflect those of the average increase in sea levels. This suggests a (highly probable) connection between the two phenomena, which is expected to continue in the future.

Floods can also occur as a consequence of tropical and extratropical cyclones. The IPCC report showed that the frequency and intensity of tropical cyclones in the North Atlantic had been increasing since the 1970s. Although the predictions of changes in intensity and frequency are highly variable on a regional basis, it is likely that tropical rainfall related to cyclones will increase with global warming. An increase in the speed of winds and the precipitation rates of tropical cyclones is expected, although this may not affect all tropical regions. The intensity of the phenomena is the most relevant aspect. In terms of extratropical cyclones, in the last 50 years, a shift toward the poles of the main extratropical cyclones has been detected for both the northern and southern hemispheres. This process is expected to continue, on average, reducing the number of cyclones at the mid-latitudes in both hemispheres.

Moreover, changes in monsoons can have implications for floods. At the moment, few studies have investigated climate change in the monsoon regions. There remains considerable uncertainty about circulation and precipitation, which does not allow for safe projections. However, the models indicate that there will be a probable increase in extreme rainfall in the monsoon regions, although not necessarily prompted by changes in monsoon characteristics and not necessarily in all monsoon regions (see, e.g., Loo et al. 2015).

Climate change is considered to have an impact on coastal areas and, consequently, on coastal floods. According to IPCC report (2014), effects of climate change are expected in terms of vulnerability of coastal areas, especially the lowlands, as a consequence of the rise in sea levels and increases in erosion. Moreover, in the absence of adaptation actions, the probability of these areas suffering negative consequences, such as coastal erosion and flooding, is high.

Floods can also result from avalanches. Changes in heat waves, glacier reduction, and permafrost degradation will have an impact on high mountain phenomena, such as slope instability, mass movements, and outburst floods in glacial lakes and rock stability (bedrock stability) (e.g., Deline et al. 2015; Stoffel and Huggel 2012; Stoffel et al. 2016). The expected effects on rainfall will have repercussions on slope movements in some areas. High mountain debris flows will begin earlier in the year due to early melting of the snowpack. The continuous degradation of permafrost and glacier retreat will reduce the stability of the rocky slopes.

About a social perspective, effects of climate change on flood features and frequency can undermine livelihood capacity especially in poor contexts (IPCC 2018; Olsson 2014). Poor people have been always more exposed to risks, as a consequence of less response capacity and marginalization. Their "confinement" in hazard-prone areas has been deeply recognized in several studies (see, e.g., Winsemius et al. 2015). Climate change is expected to increase the vulnerability of poor people as a consequence of the intensification of the episodes of extreme floods. Projections on river flood risk have been estimated (e.g., Arnell and Gosling 2016); accordingly, the episodes of current 100-year flood could double up by 2050, interesting about 450 million of people. However, the study suggests that these changes will not occur in the same way everywhere on the globe. Increases are expected in particular in tropical Africa, South and East Asia, South America, high latitude in Asia, and

North America, while decreases should take place in the Mediterranean, South West Africa, and Central Europe. Similar results have been described in IPCC reports, according to which increases in annual outflows will interest high latitudes, while reductions will occur in parts of Southern Europe, the Middle East, and Southern Africa (IPCC 2014).

Small islands states are considered to be the most vulnerable regions on the planet, and the impacts of flooding are expected to increase in these areas due to climate change. Small islands are particularly vulnerable to the average increase in sea level, since they are affected by floods, shoreline changes, and salt water infiltrations in groundwater (Kelman 2014; Mimura et al. 2007; Nunn and Kumar 2018; Ratter 2018). The contribution of the average increase in sea level to an increase in coastal high-water levels, together with the increase in the maximum wind speed of tropical cyclones, is another problem faced by small tropical island states.

While the projections (IPCC 2014) relative to the island areas differ considerably from those of the continental areas, they are characterized by considerable limitations due to the lack of data, the brevity of the observation periods, and the inadequacy of the existing climate models to represent small island territories. This is particularly evident with reference to rainfall on a global scale and with regard to the increasing number of hot days and hot nights and the decreasing number of cold days and cold nights in the Pacific and the Indian Ocean. The level of confidence for changes in the number of days/hot and cold nights is high in the case of the Caribbean, due to the greater availability of data. Changes in the oceans have repercussions on coral reefs; in particular, warming of the ocean surface has caused coral bleaching, ocean acidification, reduction of average coral growth, and reduction of oxygen concentration in the water (Seneviratne et al. 2012) with potential consequences on the flooding risk in the coastal areas.

Root Causes of Floods

According to the European Union Floods Directive (EUFD, 2007/60/EC), floods can generate damage that has important social and economic consequences for a territory. The EUFD defines floods as natural phenomena that cannot be prevented. This seems to propose the idea that there is no way to intervene except to reduce exposure. Nevertheless, the Directive recognizes that some types of human activity, such as urban planning, economic activities, hydraulic interventions, and climate change, can contribute to the impacts caused by floods. Thus, human activities can have a central role in the construction of the conditions that can lead to floods. Rufat et al. (2015) stated that several human processes form the basis of flood episodes. They include urban sprawl and, more broadly, urbanization, but also forest fires, modifications of vegetation, economic activities that destabilize the slopes, interventions of transformations and cementification on the coastline, abandonment of the slopes, no maintenance of water basins, water basin reduction interventions, destruction of natural barriers like sand dunes and mangrove forests, and granting of building abuses in areas at risk. The presence or lack of structural defenses can have a positive and negative impact on the movement of water. Moreover, aspects of social vulnerability, such as economic conditions, population distribution, and the presence of more vulnerable groups (like elderly people, persons with disabilities, low-income people, and so on), can amplify the effects of flooding and transform a hazard into a disaster.

The Behavioral Issue in Floods

During flood episodes, it is usually observed that people react incorrectly or that they are not prepared. It happens also in hazard-prone areas. Drowning is considered the principal cause of death in floods, and it is frequently consequent to wrong decisions (Becker et al. 2015). According to Becker et al. (2015), five situations induce people to entering flood waters and expose themselves to danger: undertaking recreational activities, like swimming and surfing; trying to reach a destination; recovering personal items or pets; trying to carry out work tasks; and attempting to rescue or assist

other people. These actions are consequence of risk underestimation. Thus, they are linked to personal perception of hazards.

Perception is a relevant issue in the different steps of flood risk management, from prevention to response. Misperception is usually at the basis of wrong decisions in preparedness and emergency phases. Physical and social characteristics have been analyzed with the aim of understanding which factors influence risk perception, like distance proximity to risk areas (e.g., O'Neill et al. 2016), psychological factors, socioeconomic and cultural ones, emotions and experiences, trust in institutions and rescue system (Fuchs et al. 2017; Thistlethwaite et al. 2018; also see Slovic 2016), and worry (Lechowska 2018).

According to Schad et al. (2012), misperception can depend also by a few sense of own responsibility in producing the conditions from which hazards can take place, for instance. About this, Soetanto et al. (2017) suggested that cultural, experiential, and individual factors alter the perception of social responsibility, with implications in terms of willingness to adopt resilient behaviors. A good level of risk perception does not always mean that people are willing to adopt good social protective behaviors (about this see "Risk Perception Paradox" by Wachinger et al. 2013.

Social Justice in Flood Risk Management

According to the European Commission (EC 2007), flood risk management (FRM) is the sum of all the actions taken to reduce the occurrence and impacts of floods. According to Driessen et al. (2016), studies on the topic have focused more on the natural and technical dimensions of floods. Justice is one of the topics that has received less attention (see, e.g., Johnson et al. 2007; Thaler and Hartmann 2016). Anyway, issues of social justice are central to assessing risks (Maantay and Maroko 2009). This has been partially recognized in the EU Floods Directive (2007) that refers to the need for a fair distribution of responsibilities. In scientific literature, studies of environmental justice recur in particular to the concept of vulnerability that defines who loses the most in floods and the differences in class exposure. Questions about marginalization and unequal access to security are central in flood risk management. Today, FRM must deal with the increasing exposure to flood risk and with the limits of a government's capacity to respond to these hazards. Considering the increase of the areas exposed to flood risk, political choices must be made to decide where and if interventions should occur, and the relevant implications of those decisions must be addressed in terms of distributive justice (see Johnson et al. 2007). Concept of justice differs in every country and can have different implications on the way of allocating and distributing protective solutions (Thaler and Hartmann 2016).

Measures for flood protection can have implications on the vulnerability distribution, with, e.g., consequences on the property values and on the level of exposure. These choices can be at the basis of gentrification processes (see the case of New Orleans after Katrina hurricane) and social conflicts, and they can be interpreted as violations of the social contract (Zografos 2017). The social contract bases on the idea that citizens are obedient to the state in exchange for security. So the state is asked to guarantee social security. When the condition of security is lost or is perceived as reduced or lost, in particular in case of disasters, the validity of the social contract is challenged. A discussion of the social contract may produce the loss of social control by the state and governmental inability to continue to guarantee social security for the future.

Conclusion

Floods are situations of overflowing in dry areas that can happen suddenly or slowly and with different impacts. They can be classified according to different characteristics, like magnitude, location, and impacts. Most relevant differences are identified between coastal and river floods. Climate change has been expected to have impacts on frequency and intensity of floods as a consequence of different kinds of climatic phenomena, like cyclones, rainfalls, and sea

level rise. Small islands are the most vulnerable areas exposed in particular to sea flooding.

The origin of floods usually can be traced to human interventions that altered the natural water system. Many human activities have implications on flooding occurrence, and they are responsible for disaster consequences. Also the measures adopted to reduce flood risk can have consequences in terms of vulnerability and implications for social justice.

Cross-References

- ▶ Federal Emergency Management Agency
- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
- ▶ Natural Hazards
- ▶ Natural Hazards: Hurricanes, Cyclones, and Typhoons

References

Alexander, D. (1997). The study of natural disasters, 1977–97: Some reflections on a changing field of knowledge. *Disasters, 21*(4), 284–304.

Arnell, N. W., & Gosling, S. N. (2016). The impacts of climate change on river flood risk at the global scale. *Climatic Change, 134*(3), 387–401.

Becker, J. S., Taylor, H. L., Doody, B. J., Wright, K. C., Gruntfest, E., & Webber, D. (2015). A review of people's behavior in and around floodwater. *Weather, Climate, and Society, 7*(4), 321–332.

Berghuijs, W. R., Aalbers, E. E., Larsen, J. R., Trancoso, R., & Woods, R. A. (2017). Recent changes in extreme floods across multiple continents. *Environmental Research Letters, 12*(11), 114035.

Blöschl, G., Hall, J., Parajka, J., Perdigão, R. A., Merz, B., Arheimer, B., et al. (2017). Changing climate shifts timing of European floods. *Science, 357*(6351), 588–590.

Box, P., Bird, D., Haynes, K., & King, D. (2016). Shared responsibility and social vulnerability in the 2011 Brisbane flood. *Natural Hazards, 81*(3), 1549–1568.

Deline, P., Gruber, S., Delaloye, R., Fischer, L., Geertsema, M., Giardino, M., … & McColl, S. (2015). Ice loss and slope stability in high-mountain regions. In *Snow and ice-related hazards, risks and disasters* (pp. 521–561). Amsterdam: Academic Press.

Driessen, P. P., Hegger, D. L., Bakker, M. H., van Rijswick, H. F., & Kundzewicz, Z. W. (2016). Toward more resilient flood risk governance. *Ecology and Society, 21*(4), 53.

European Floods Directive (EC) (2007). On the assessment and management of flood risks. 23 October 2007. Off J Eur Union, L 288.

FEMA (2018). *Flood or flooding*. https://www.fema.gov/flood-or-flooding

Fischer, S., & Schumann, A. (2018). A distribution-free ordinal classification of floods based on moments. *Hydrological Sciences Journal, 63*(11), 1605–1618.

Fuchs, S., Karagiorgos, K., Kitikidou, K., Maris, F., Paparrizos, S., & Thaler, T. (2017). Flood risk perception and adaptation capacity: A contribution to the socio-hydrology debate. *Hydrology and Earth System Sciences, 21*(6), 3183–3198.

Hewitt, K. (2014). *Regions of risk: A geographical introduction to disasters* (p. 410). London: Routledge.

IPCC (2014). *Climate change 2014: Impacts, adaptation, and vulnerability. Part A: Global and sectoral aspects. Contribution of Working Group II to the fifth assessment report of the Intergovernmental Panel on Climate Change*. Switzerland: IPCC, Geneva.

Johnson, C. L., Penning-Rowsell, E., & Parker, D. (2007). Natural and imposed injustices: The challenges in implementing 'fair' flood risk management policy in England. *The Geographical Journal, 173*(4), 374–390. https://doi.org/10.1111/j.1475-4959.2007.00256.x.

Koks, E. E., Jongman, B., Husby, T. G., & Botzen, W. J. (2015). Combining hazard, exposure and social vulnerability to provide lessons for flood risk management. *Environmental Science & Policy, 47*:42–52.

Karagiorgos, K., Thaler, T., Hübl, J., Maris, F., & Fuchs, S. (2016). Multi-vulnerability analysis for flash flood risk management. *Natural Hazards, 82*(1), 63–87.

Kuhlicke, C., Scolobig, A., Tapsell, S., Steinführer, A., & De Marchi, B. (2011). Contextualizing social vulnerability: Findings from case studies across Europe. *Natural Hazards, 58*(2), 789–810.

Kundzewicz, Z. W., Pińskwar, I., & Brakenridge, G. R. (2013). Large floods in Europe, 1985–2009. *Hydrological Sciences Journal, 58*(1), 1–7.

Kvočka, D., Falconer, R. A., & Bray, M. (2016). Flood hazard assessment for extreme flood events. *Natural Hazards, 84*(3), 1569–1599.

Lechowska, E. (2018). What determines flood risk perception? A review of factors of flood risk perception and relations between its basic elements. *Natural Hazards, 94*(3), 1341–1366.

Lee, D., et al. (2018). Impacts of half a degree additional warming on the Asian summer monsoon rainfall characteristics. *Environmental Research Letters, 13*(4), 044033. https://doi.org/10.1088/1748-9326/aab55d.

Loo, Y. Y., Billa, L., & Singh, A. (2015). Effect of climate change on seasonal monsoon in Asia and its impact on the variability of monsoon rainfall in Southeast Asia. *Geoscience Frontiers, 6*(6), 817–823.

Maantay, J., & Maroko, A. (2009). Mapping urban risk: Flood hazards, race, & environmental justice in New York. *Applied Geography, 29*(1), 111–124.

Mavhura, E., Manyena, B., & Collins, A. E. (2017). An approach for measuring social vulnerability in context: The case of flood hazards in Muzarabani district, Zimbabwe. *Geoforum, 86*, 103–117.

Mimura, N., Nurse, L., McLean, R., Agard, J., Briguglio, L., Lefale, P., … & Sem, G. (2007). Small islands. *Climate change*, *16*, 687–716.

Montz, B. E., & Tobin, G. A. (2011). Natural hazards: An evolving tradition in applied geography. *Applied Geography, 31*(1), 1–4.

Nasiri, H., Yusof, M. J. M., & Ali, T. A. M. (2016). An overview to flood vulnerability assessment methods. *Sustainable Water Resources Management, 2*(3), 331–336.

Nunn, P., & Kumar, R. (2018). Understanding climate-human interactions in Small Island Developing States (SIDS) implications for future livelihood sustainability. *International Journal of Climate Change Strategies and Management, 10*(2), 245–271.

Olsson, L., et al. (2014). Livelihoods and poverty. In C. B. Field, V. R. Barros, D. J. Dokken, K. J. Mach, M. D. Mastrandrea, T. E. Bilir, M. Chatterjee, K. L. Ebi, Y. O. Estrada, R. C. Genova, B. Girma, E. S. Kissel, A. N. Levy, S. MacCracken, P. R. Mastrandrea, & L. L. White (Eds.), *Climate change 2014: Impacts, adaptation, and vulnerability. Part A: Global and sectoral aspects. Contribution of working group II to the fifth assessment report of the intergovernmental panel on climate change* (pp. 798–832). Cambridge/New York: Cambridge University Press.

O'Neill, E., Brereton, F., Shahumyan, H., & Clinch, J. P. (2016). The impact of perceived flood exposure on flood-risk perception: The role of distance. *Risk Analysis, 36*(11), 2158–2186.

Oulahen, G., Mortsch, L., Tang, K., & Harford, D. (2015). Unequal vulnerability to flood hazards: "Ground truthing" a social vulnerability index of five municipalities in Metro Vancouver, Canada. *Annals of the Association of American Geographers, 105*(3), 473–495.

Pesaresi, M., Ehrlich, D., Kemper, T., Siragusa, A., Florczyk, A.J., Freire, S., & Corbane, C. (2017). Atlas of the Human Planet 2017: Global exposure to natural hazards. EUR 28556 EN, https://doi.org/10.2760/19837.

Ratter, B. M. (2018). Island vulnerability and resilience. In *Geography of Small Islands* (pp. 173–199). Cham: Springer.

Rufat, S., Tate, E., Burton, C. G., & Maroof, A. S. (2015). Social vulnerability to floods: Review of case studies and implications for measurement. *International Journal of Disaster Risk Reduction, 14*, 470–486.

Sayers, P., Penning-Rowsell, E. C., & Horritt, M. (2018). Flood vulnerability, risk, and social disadvantage: Current and future patterns in the UK. *Regional Environmental Change, 18*(2), 339–352.

Schad, I., Schmitter, P., Saint-Macary, C., Neef, A., Lamers, M., Nguyen, L., Hilger, T., & Hoffmann, V. (2012). Why do people not learn from flood disasters? Evidence from Vietnam's northwestern mountains. *Natural Hazards, 62*(2), 221–241.

Seneviratne, S. I., Nicholls, N., Easterling, D., Goodess, C. M., Kanae, S., Kossin, J., Luo, Y., Marengo, J., McInnes, K., Rahimi, M., Reichstein, M., Sorteberg, A., Vera, C., & Zhang, X. (2012). Changes in climate extremes and their impacts on the natural physical environment. In C. B. Field, V. Barros, T. F. Stocker, D. Qin, D. J. Dokken, K. L. Ebi, M. D. Mastrandrea, K. J. Mach, G.-K. Plattner, S. K. Allen, M. Tignor, & P. M. Midgley (Eds.), *Managing the risks of extreme events and disasters to advance climate change adaptation* (A special report of working groups I and II of the Intergovernmental Panel on Climate Change (IPCC)) (pp. 109–230). Cambridge/New York: Cambridge University Press.

Slovic, P. (2016). *The perception of risk*. London Routledge.

Soetanto, R., Mullins, A., & Achour, N. (2017). The perceptions of social responsibility for community resilience to flooding: The impact of past experience, age, gender and ethnicity. *Natural Hazards, 86*(3), 1105–1126.

Stoffel, M., & Huggel, C. (2012). Effects of climate change on mass movements in mountain environments. *Progress in Physical Geography, 36*(3), 421–439.

Stoffel, M., Wyżga, B., Niedźwiedź, T., Ruiz-Villanueva, V., Ballesteros-Cánovas, J. A., & Kundzewicz, Z. W. (2016). Floods in mountain basins. In *Flood risk in the Upper Vistula Basin* (pp. 23–37). Cham: Springer.

Thaler, T., & Hartmann, T. (2016). Justice and flood risk management: Reflecting on different approaches to distribute and allocate flood risk management in Europe. *Natural Hazards, 83*(1), 129–147.

Thistlethwaite, J., Henstra, D., Brown, C., & Scott, D. (2018). How flood experience and risk perception influences protective actions and behaviours among Canadian homeowners. *Environmental Management, 61*(2), 197–208.

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). The risk perception paradox—Implications for governance and communication of natural hazards. *Risk Analysis, 33*(6), 1049–1065.

White, G. F. (1945). Human adjustment to floods. Unpublished PhD, Department of Geography, University of Chicago.

Winsemius, H. C., Jongman, B., Veldkamp, T. I., Hallegatte, S., Bangalore, M., & Ward, P. J. (2015). *Disaster risk, climate change, and poverty: Assessing the global exposure of poor people to floods and droughts*. World Bank Policy Research Working Paper 7480 (November):1–35.

Zografos, C. (2017). Flows of sediment, flows of insecurity: Climate change adaptation and the social contract in the Ebro Delta, Catalonia. *Geoforum, 80*, 49–60.

Further Reading

Alexander, M., Priest, S., & Mees, H. (2016). A framework for evaluating flood risk governance. *Environmental Science & Policy, 64*, 38–47.

Kim, H., Marcouiller, D. W., & Woosnam, K. M. (2018). Rescaling social dynamics in climate change: The implications of cumulative exposure, climate justice, and community resilience. *Geoforum, 96*, 129–140.

O'Hare, P., & White, I. (2018). Beyond 'just' flood risk management: The potential for—and limits to—alleviating flood disadvantage. *Regional Environmental Change, 18*(2), 385–396.

Terti, G., Ruin, I., Anquetin, S., & Gourley, J. J. (2015). Dynamic vulnerability factors for impact-based flash flood prediction. *Natural Hazards, 79*(3), 1481–1497.

Natural Hazards: Hurricanes, Cyclones, and Typhoons

Gary A. Gordon[1] and Richard R. Young[2]
[1]Emergency Management Department, Massachusetts Maritime Academy, Buzzards Bay, MA, USA
[2]School of Business Administration, Capital College, The Pennsylvania State University, Middletown, PA, USA

Keywords

Natural disasters · Hurricanes, cyclones, and typhoons · Emergency preparedness and management · Cascading effects · Homeland security · Mitigation

Definition

Hurricanes and typhoons are tropical cyclones with different origins and areas of impact. They are meteorological natural disasters that have significant impacts, could have cascading effects, and could be exploited for terror purposes.

Introduction

Hurricanes, cyclones, and typhoons in the context of security and emergency management go beyond a simple definition. They must be looked at not just from the physical characteristics and potential devastation, but holistically with regard to cascading events, resiliency, and homeland security impacts.

Simply, *hurricanes* are tropical cyclones that originate in the Atlantic Basin (typically the Atlantic Ocean, Caribbean Sea, and Gulf of Mexico) and the eastern and central North Pacific Ocean. *Typhoons* are tropical cyclones typically in the Northwest Pacific. *Tropical cyclone* nomenclature is typically used for storms that are in the South Pacific and Indian Ocean. Hence, geographical location determines what the storm is called (NOAA 2018). They are categorized by wind speed via the Saffir-Simpson scale ranging from Category 1 storms with sustained wind speeds of 74–95 miles per hour (MPH) to Category 5 (157 MPH or higher). (The Saffir-Simpson hurricane wind scale is based on a hurricane's sustained wind speed that reflects potential property damage and is categorized as major (Category 3 and higher) because of the potential for significant loss of life and damage.) Category 3–5 storms are considered major (NHC 2018). Table 1 is a graphic representation of the Saffir-Simpson scale showing damage potential.

Whether a hurricane or typhoon, the storms are rotating low-pressure systems containing thunderstorms with no clear delineation between the air masses. They start as tropical depressions with wind speeds of less than 39 MPH. They

Natural Hazards: Hurricanes, Cyclones, and Typhoons, Table 1 Saffir-Simpson scale

Category	Sustained winds (MPH)	Wind damage
1	74–95	Very dangerous winds producing some damage
2	96–110	Extremely dangerous winds causing extensive damage
3	111–129	Devastating damage will occur
4	130–156	Catastrophic damage will occur
5	>157	Catastrophic damage will occur

Source: (NHC 2018)

become tropical storms when wind speeds exceed 39 MPH but are less than 75 MPH, when the storm becomes a hurricane, typhoon, or tropical cyclone.

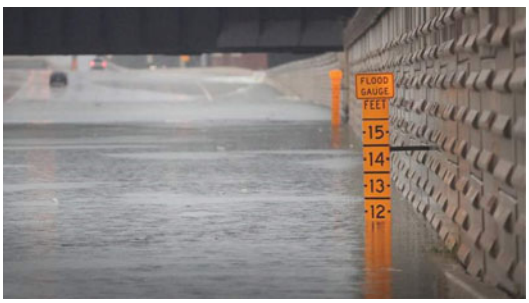
Characteristics

These storms are characterized by wind, rain, storm surge, and flooding, all of which cause damage. The wind causes damage to structures and frequently causes widespread power outages. Wind and the width of the wind field is a factor in storm surge and causes additional damage, such as that experienced with the 2005 Hurricane Katrina levee failures. Rain and flooding, as experienced with Hurricane Harvey in Texas in 2017 with its more than 50″ of rainfall, resulted in the failure of the Addicks and Barker dams, which are flood control structures located in the City of Houston (Rogers 2017). The dam failures, like other similar rain and flooding events, could cause extensive damage, casualties, contamination of drinking water, and a range of environmental issues.

The effects of wind as measured by the Saffir-Simpson scale includes estimates of expected damage. For example, a Category 2 hurricane with winds of between 96 and 110 MPH can be expected to cause extensive damage. This equates to well-constructed homes sustaining major roof and siding damage, shallow-rooted trees could be snapped or uprooted, and numerous roads could be blocked (NHC 2018). As we have seen from Hurricanes Irma and Maria in Puerto Rico in 2017, extensive and lengthy power outages can result.

The effects of hurricane, typhoon, and tropical cyclone rains are dependent on many factors. Rain, when considering intensity and surface conditions (soil and imperviousness) when combined with wide wind fields and storm surge, can cause extensive flooding. The impacts are at the mercy of the intersection of the built and natural environment and could cause both personal and economic impacts. Drainage and flood control structures, such as levee walls, seawalls, and dams, are important in mitigating the impact of rain, storm surge, and flooding. What and how one builds in flood-prone areas is important. In Houston, for example, many highway underpasses are depressed; hence they flood easily. (It is standard and widely accepted civil engineering practice to elevate or depress road crossings at a major highway. This is because local and regional/county roads often predate the major highway. Adjacent land use, topography, soil conditions, water table, and construction costs are among the factors that "drive" the elevation of the major highway, its entrances and exits, and whether or not the crossroads are elevated or depressed. In Houston, these conditions are prevalent requiring the depression of many crossroads, highway entrances and exits, and turnarounds. This condition is not unique to Houston and can be found throughout the country.) The photo below in Fig. 1 shows how that when the elevation under the highway must be depressed, the general public can be made aware of the potential flooding with the associated danger.

There is much discussion that there is a link between global warming and more frequent and stronger hurricanes. Global climate models suggest that greenhouse gases can cause ocean warming, but observational data suggests that the warming may not be as extensive as suggested (Landsea 2011). Hurricanes, typhoons in the Northwest Pacific, and severe tropical cyclones in the Indian and Southwest Pacific have been destructive and responsible for mass casualties and extensive property damage. Landsea suggests that ocean temperature is not the only factor that



Natural Hazards: Hurricanes, Cyclones, and Typhoons, Fig. 1 Typical Underpass Flood Cage. Source: (Cleary 2017)

causes disturbances to become tropical storms, hurricanes, and typhoons. Moist air, thunderstorms, and wind shear are also contributors. Climate models posit that there is a 2-degree warming of the air for every degree of ocean warming (Thomas Knutson 2004).

How does this affect hurricanes, typhoons, and tropical cyclones? Modelling suggests that hurricanes, typhoons, and tropical cyclones may be slightly stronger by the end of this century. Moreover, the climate models also suggest that the number of tropical storms, hurricanes, typhoons, and tropical cyclones will not go up and may perhaps even decrease, which could be attributed to wind shear.

What does this mean today? With the predicted 1°F increase in ocean temperature, hurricanes, typhoons, and tropical cyclones may experience a similar increase in intensity. Using the Saffir-Simpson scale, a Category 5 hurricane would produce a 1–2 MPH increase in wind speed. Landsea opines that hurricanes, typhoons, and tropical cyclones are stronger due to global warming, but it is inconclusive as to the magnitude. A 1–2 MPH increase in intensity is small and not measurable by aircraft and satellites (Landsea 2011).

Landsea further states that it is not surprising that many have concluded that damage and losses are comparable to the anticipated rise in ocean temperature. However, this is not necessarily the case and does not consider other factors that cause damages. Two of these include (1) people have more money now than in the past resulting in more expensive housing and personal property and (2) that people choose to live near the coast. What does this mean? People are willing to accept risk, but preparedness, mitigation, and forecasting and tracking can offset that risk.

Hurricanes, Nor'easters and Winter Storms

Hurricanes can occur in many forms and include a combination of weather patterns and events to create unique storm events year round (Pereria 2018). They include:

- *Bomb cyclones* or *bomb*s, which are characterized by the rapid intensification of a cyclone far offshore with or without heavy snow.
- Winter hurricanes, which are *extratropical cyclones* outside of the tropics, but are simply a winter storm that may have hurricane winds offshore.
- *Nor'easters* are storms that run up the East Coast with maximum intensity impacting New England and the Canadian Maritime Provinces.
- *Blizzards* are winter storms with tropical storm winds lasting for a period of 3 hours more.

Hurricane or Superstorm Sandy, for example, was a meteorological anomaly and special type of storm. It wrapped cold air around an intact, tropical warm core and has been considered to be the combination and confluence of a hurricane and Nor'easter resulting in extensive and widespread damage in the Northeast (Halverson 2013).

Over a 3-week period in February and March 2018, four consecutive Nor'easters impacted the Mid-Atlantic and Northeast states. These storms were characterized by high winds, heavy snowfall, and extensive coastal flooding. Extensive and prolonged power outages were experienced, which could have been exploited by those seeking to increase the devastation for terror purposes. These storms are typical of Northeast winters, but the intensity, frequency, and timing were significant. Research is being conducted to examine the storm events and trends (Liberto 2018).

What Are the Natural Impacts?

Hurricane, typhoon, or tropical cyclone damage is not only from wind. It occurs as the result of, among other things, rainfall, storm surge and flooding, and resulting impacts. Storm surge and flooding post Hurricane Katrina in 2005 combined with pollutants from, among other things, chemical plants and waste water treatment facilities was thought to have created a "toxic soup." However, research by Louisiana State University, the Louisiana Department of Environmental Quality and American Chemical Society, found that the floodwaters were not nearly as toxic and

concluded that it was more like drainage experienced after a heavy rainfall (Marris 2006).

Hurricane Harvey in 2017 caused extensive flooding in the Houston metropolitan area associated with a 50″ rainfall over several days. Dam releases, much like the failure of the levee walls in New Orleans during Hurricane Katrina, were a major source of devastation exacerbating the extensive rainfall and storm surge. So, the failure of constructed facilities can worsen the damage directly attributable to wind, rain, and flooding associated with a hurricane, typhoon, and tropical cyclone.

Forecasting and Tracking and Preparedness

Forecasting and tracking and preparedness measures are key factors that reduce risk and, ultimately, loss of life and damage. As was seen with the recent preparation for Hurricane Florence (occurred during mid-September 2018), people are given ample time to prepare their homes and business and evacuate to a safe location. You also see government agencies and volunteer organizations stage and safely preposition assets to immediately assist in the response. Power companies and other utilities also stage repair crews and prepare their facilities to minimize damage and recover as soon as feasibly possible. Forecasting and tracking and preparedness have come a long way since Hurricane Katrina.

Forecasting and tracking is not just from the National Hurricane Center but comes from independent weather companies, such as The Weather Channel, the meteorology departments of major research universities, and local and national television companies. The use of aircraft and satellites has helped by providing visual and electronic data that is used in the forecasting and tracking. A range of different computer model developments has dramatically improved research and forecasting activities.

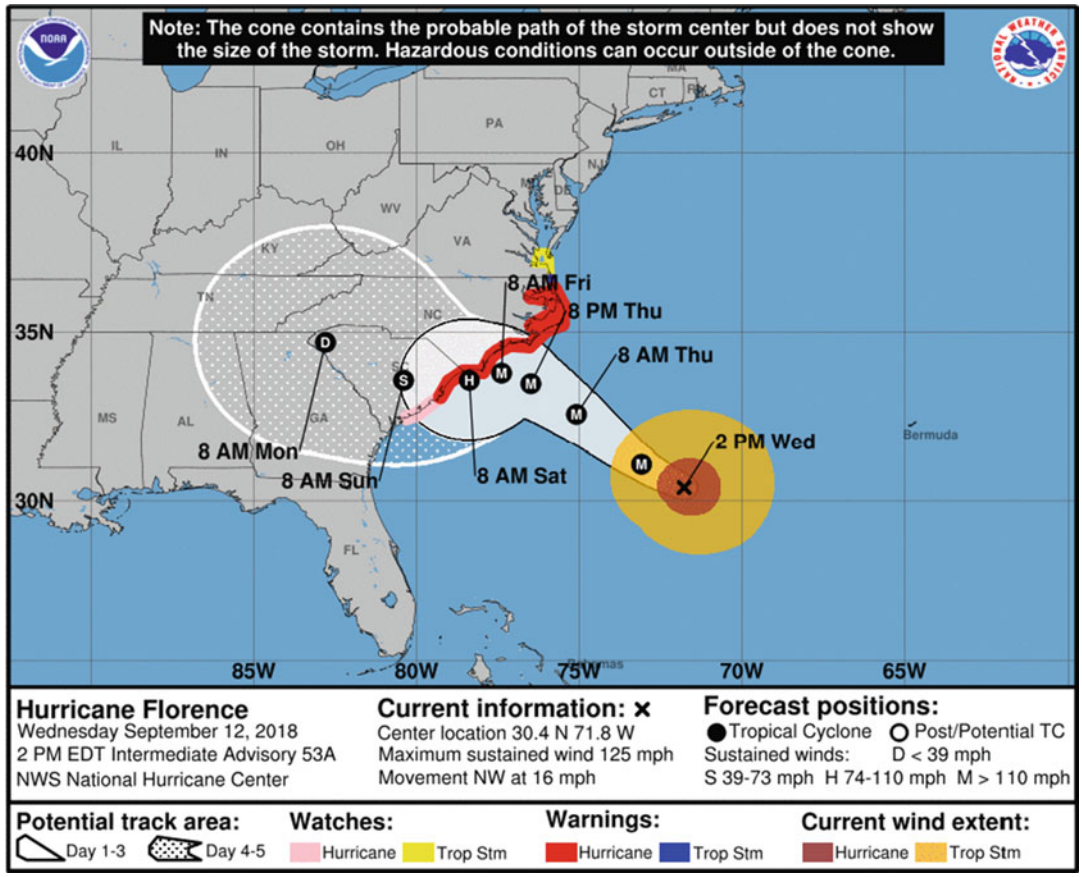
There are several kinds of forecast models. *Dynamic models* look at the physics and motion of the atmosphere, while *statistical models* are based on past hurricane data. These models can be blended into *statistical-dynamic models* that use historical data from both storm behavior and atmospheric variables to develop forecasts. *Trajectory models* move a hurricane, typhoon, and tropical cyclone along a forecasted track based on the wind field. *Ensemble models* use forecasts from different models, physical conditions, and/or initial conditions to create a blended forecast. *Numerical models* of storm surge, waves, and coastal flooding are used to forecast landfall impacts, rather than track and intensity (University of Rhode Island 2018).

Research models are designed to simulate the behavior of a hurricane, typhoon, and tropical cyclone but are not necessarily intended to make forecasts. These models are generally more complex and data intensive than *forecast models*. *Research models*, however, have been known to be used to forecast hurricanes, typhoons, and tropical cyclones or improve on existing models. Hurricane research and *forecast models* are focused on making the 3–5-day forecasts in addition to, along with climate models, predicting future hurricane activity (University of Rhode Island 2018). Figure 2 is a forecast track with cone of uncertainty that is typically used during the preparedness phase.

Cascading Impacts

Cascading events occur as a direct or indirect result of a man-made or natural disaster (FEMA 2013). Power outages caused by hurricanes, blizzards, or earthquakes are examples of cascading effects. An oil spill caused by a truck accident on an icy road during a winter storm is another. *NaTechs* (Natural and technological disasters) are those cascading events whereby a natural disaster causes a technological disaster (Brenda Phillips 2017).

A classic example of a disaster with cascading effects, the Fukushima Daiichi nuclear power plant disaster in 2011 is a common example of a NaTech. The disaster is the result of an earthquake in the Pacific Ocean that caused a tsunami that disabled the emergency generators resulting in a failure of the ability to cool the reactors. A power outage resulting from a hurricane, typhoon, or blizzard is a cascading event and is considered a NaTech by many. A difference, however, is that damage to power distribution systems from a hurricane, typhoon, or blizzard is



Natural Hazards: Hurricanes, Cyclones, and Typhoons, Fig. 2 National Hurricane Center Forecast Track Example. Source: (NWS 2018)

expected, but a Fukushima Daiichi disaster is not (communications and power outage, although technically NaTechs, by definition, are expected results of certain disasters (e.g., Nor'easter and hurricane) and are predictable consequences. NaTechs can be considered as aberrations and not an expected result of a natural disaster. The Fukushima Daiichi nuclear power plant catastrophe (earthquake, tsunami, and power plant disaster), for example, was an unexpected event commonly thought of as a NaTEch.).

Some say that power and communications outages are NaTechs. From the perspective of cascading events or anticipated results, they are expected and are not a low likelihood event like the Fukushima Daiichi disaster. Consider, for example, the 2018 late winter Nor'easters or even the 2015 snow season in the Northeast, which resulted in extensive power outages, but it was expected, and resources were staged so as to respond as soon as possible. Metropolitan Boston, New Orleans, Houston, and South Carolina should now be considering power outages a cascading effect from a hurricane or tropical storm and resulting storm surge and flooding.

Let's look at Hurricane Harvey in 2017. This Category 4 hurricane was quickly downgraded to a tropical storm after landfall. Given its location and hurricane experience, Houston prepared for the storm, but the prolonged rain and extensive flooding was not anticipated. Because of the heavy rains, Barker and Addicks reservoirs, which are used to control flooding in downtown Houston, had to have controlled releases causing

damage downstream (Rick Jervis 2017). Similar scenarios were experienced with the levee failures from Hurricane Katrina in 2005 – such eventualities should be considered during planning, mitigation, and preparedness.

What Are the Security Concerns?

When considering and preparing for hurricanes, the focus is on safety and preservation of life and property. But the protection of people and property from the exploitation of a natural disaster must also be considered. A terrorist could target the evacuees and first responders, among others, as they flee from or respond to a natural disaster. Not just people, the objective could be a business or government agency being targeted for sabotage. For example, as Hurricane Rita approached Texas, the Department of Homeland Security (DHS) received an alert of a potential attack on railcars containing hazardous material along the Gulf Coast when everyone was otherwise hunkered down. A successful attack could have been clearly catastrophic exacerbating the impact of the hurricane. Fortunately nothing occurred.

Some other security considerations associated with hurricanes, typhoons, and tropical cyclones involve power outages, loss of communications, compromised access via road and bridge outages, and environmental problems. With regard to power outages, access and perimeter control could be inoperable unless an alternate power supply is readily available. This is important at transportation facilities and, in particular, airports. Communications systems are dependent on power. Even with power, they could be impacted resulting in the inability of alarm systems to operate. In addition to airports, other infrastructure has alarm systems not the least of which is the nation's nuclear power plants. Other potential exploitations might occur when there is no power or communications, such as the potential interdiction at a water treatment plant to contaminate the water supply, introduction of a bio/chem agent in an out of service transportation terminal, such as South Station in Boston, and placing an improvised explosive device (IED) in a major hospital emergency room. These were scenarios considered during and after Hurricanes Katrina, Rita, and Ike.

With roads and bridges out, a terrorist group could conduct an active shooter event or explode an IED at many venues, to including an evacuation shelter, with the knowledge that law enforcement and first responders may not be able to respond quickly. It is a time when everyone is focused on the immediate protection and saving and preserving life and property from the hurricane, typhoon, or tropical cyclone. The range of environmental issues can include an oil spill resulting from storm surge and flood waters and overflow of a chemical plant or wastewater treatment facility. If the disaster does not do this, then a terrorist could take advantage of conditions and manually open oil, sewer, and/or chemical plant lines.

In the above potential scenarios, what may have been considered a hardened target may now become a soft target. This concept can be applied to any infrastructure and operating system post landfall.

How to Prepare and Mitigate

The issue with hurricanes, typhoons, and tropical cyclones is the intersection of the built environment and nature that creates the disaster. Development on the coast, in flood-prone areas, and along estuaries creates the intersection. We, as a society, enjoy living near the coast and accept the risk. Mitigation measures are the responsibility of not only government agencies, but that of the home and/or business owners. Structural and nonstructural measures are the methods of mitigation that are the most prevalent.

Structural mitigation measures include, at the government level, levee walls, seawalls, and storm drainage systems. These also include resilient structures that provide municipal services, to include power, water, and waste water treatment. For a building or homeowners, this means designs that have floor elevations above flood level, stable roofs (via "hurricane clamps"), and resilient foundations and structures.

Nonstructural mitigation measures at the government level include zoning ordinances and building codes that restrict where and how to build

and acquiring land susceptible to flooding by eminent domain. Home and business owners can mitigate the effect of hurricanes, typhoons, and tropical cyclones by using flood zones as parks and parking areas, flood insurance, and voluntary relocating out of hurricane and storm surge-prone areas.

Conclusion

When considering hurricane, tropical cyclone, and typhoon preparedness, an all-hazards approach needs to be taken. Such includes the protection of life and property and the protection of the evacuees and first responders from cascading affects and exploitation. Therefore, emergency managers and professionals should not just consider the hurricane, tropical cyclone, or typhoon at hand, but need to consider what could happen after landfall. They should prepare for cascading events so that a Fukushima Daiichi does not happen or a potential exploitation like that which could have occurred along the Gulf Coast as Hurricane Rita approached can be avoided.

Power outages are common with many of these storms, and approaches to minimizing them should be a major focus. Infrastructure resilience and proper mitigation measures are important. Presidential Policy Directive (PPD) 21 identifies the power or energy sector as critical because it is an "enabling function" across all of the 16 critical infrastructure sectors (Energy Sector 2018). Without power or energy, response and recovery is made significantly more difficult.

Cross-References

- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Recent Incidents That Contributed to Changes in Emergency Management Legislation and Procedures
- ▶ Natural Hazards
- ▶ Natural Hazards: Hurricanes, Cyclones, and Typhoons

References

Brenda Phillips, D. N. (2017). Introduction of emergency management (2nd ed.). Boca Raton, FL: CRC Press/ Taylor & Francis Group.

Cleary, T. (2017, August 27). *Houston rainfall totals for Hurricane Harvey.* Retrieved from Heavy.com: https://heavy.com/news/2017/08/houston-rain-rainfall-totals-harvey-amount-flooding-august-27-today/

Energy Sector. (2018, September 12). Retrieved from DHS: https://www.dhs.gov/energy-sector

FEMA. (2013). *IS-230, Fundamentals of emergency management*.

Halverson, J. (2013, October 29). Superstorm Sandy: Unraveling the mystery of a meteorological oddity. *The Washington Post*.

Landsea, C. (2011, November). *Hurricanes and global warming.* Retrieved from NOAA: www.aoml.noaa.gov/hrd/Landsea/gw_hurricanes/index.html

Liberto, T. D. (2018, March 14). *Climate.gov.* Retrieved from https://www.climate.gov/print/831355

Marris, E. (2006). New Orleans cleared of 'toxic soup' scenario. *Nature: International Journal of Science*. Published online on: 15 Sep 2006

NHC. (2018, July 27). Retrieved from Saffir-Simpson Hurricane Wind Scale: https://www.nhc.noaa.gov/aboutsshws.php

NOAA. (2018, July 17). Retrieved from What is the difference between a hurricane and a typhoon?: https://oceanservice.noaa.gov/facts/cyclone.html

NWS. (2018, September 12). *National Hurricane Center.* Retrieved from https://www.nhc.noaa.gov/

Pereria, S. (2018, January 3). Are bomb cyclones real? The difference between a Nor'Easter, Blizzard and a Winter Hurricane. *Newsweek*.

Rick Jervis, D. R. (2017, August 28). Release of reservoir water could affect thousands in Houston area. *USA Today.*

Rogers, A. (2017, August 31). With Harvey, imperfect engineering meets a perfect storm. *Science*.

Thomas Knutson, R. T. (2004). Induced warming on simulated hurricane intensity and precipitation: sensitivity to choice of climate model and convective parameterization. *Journal of Climate, 17*(18):3477–3495

University of Rhode Island. (2018, September 12). Retrieved from Hurricanes: Science and Society: http://www.hurricanescience.org/science/forecast/

Further Reading

Conger, J. (2018, November 1). *Hurricane Florence's impacts on military installations and missions in the Southeast*. The Center for Climate and Security. https://climateandsecurity.org/

FEMA. (2018). *Natural disasters*. https://www.dhs.gov/natural-disasters

International Air Transport Association. (2017, November). *Assessment of Hurricane Irma and Maria's impacts on aviation*. https://www.iata.org/

publications/economics/Reports/Impact-of-Hurricanes-Irma-and-Maria.pdf.
International Atomic Energy Agency. (2018). *Fukushima Daiichi Status Updates*. https://www.iaea.org/newscenter/focus/fukushima/status-update
NHC. (2018). *Storm Surge overview.* https://www.nhc.noaa.gov/surge/
Young, R., Gordon, G., & Plant, J. (2017). Chapter 10 Emergency or incident response, operations, and security. In *Railway security: Protecting against manmade and natural disasters*. New York: Routledge.

Natural Hazards: Pandemic Threats by Infectious Diseases

Peter Mameli
Public Management, John Jay College of Criminal Justice, New York, NY, USA

Keywords
Center for Disease Control · Disease outbreaks · Global health · Infectious diseases · Plague · Public health · WHO/World Health Organization

Definition

Human hazard: Threats to human populations where the authentic source of the occurrence is technological or human made.

Natural hazard: Threats to human populations where the authentic source of the occurrence is found in the natural world. Biological natural hazards include the ecological emergence of infectious disease.

Pandemic: The global outbreak of an infectious disease where no vaccine, or natural resistance, exists that is able to stabilize the threat.

Introduction

In 2018 the World Health Organization (WHO) identified a group of priority diseases and pathogens for research and development purposes in the years ahead. Each one represents a unique threat to public health, although it cannot be said with certainty that large-scale outbreaks will necessarily occur. These threats either have no current countermeasures or countermeasures that are known to be lacking for preventing spread of illness. The list included Crimean-Congo hemorrhagic fever (CCHF), Ebola virus disease and Marburg virus disease, Lassa fever, Middle East respiratory syndrome coronavirus (MERS-CoV) and severe acute respiratory syndrome (SARS), Nipah and henipaviral diseases, Rift Valley fever (RVF), Zika, as well as Disease X (World Health Organization 2018a).

Disease X holds a special place on the list, for it reflects an understanding that catastrophic infectious diseases are far from comprehensively identified at this point in time. As such the possibility of new pandemics emerging is not far-fetched, but quite conceivable.

There has been disagreement about what the term "pandemic" should encompass for many years. One concise definition posits that a global outbreak of a novel disease is necessary to invoke the word (World Health Organization 2010). Less compact explanations suggest pandemics involve countrywide spread at the very least or consider regional impact on one or more continents as acceptable for the term to be applied. In any nuanced discussion, case levels are usually seen as being considerable, and immunity limited. For the purposes of this submission, the World Health Organization approach offered above will be employed. As a result of accepting this definition, the review to follow keys more on international, rather than regional, national, local, and individual approaches to these types of public health threats.

New pandemics are not the only health concerns people around the globe must remain vigilant over, however. The reemergence and tenacity of plague in disparate locations around the globe, as well as continuing battles with HIV/AIDS and new strains of influenza, are but three established infectious diseases that stubbornly stalk human populations. Further still, there remains a seemingly relentless nature to illnesses such as tuberculosis, malaria, yellow fever, cholera, syphilis, and gonorrhea. Combined with the steady onslaught of a range of slow-acting chronic diseases, global public health crises of all kinds promise to continually impact

and even shape the course of human development as time moves on. Pandemic threats are simply one type among them.

Although not the focus of a piece on natural pandemic threats, due to the technological or human-made intervention that leads to their spread, the ongoing specter of biological warfare or terrorism releasing some uncontrolled deadly pathogen on the planet must at least bear mention in this discussion. In addition industrial accidents also present the human population with an array of outbreak possibilities, both at the time of occurrence as well as during the aftermath of crisis. Recognizing the full breadth of infectious disease threats that can become global is important because innovations from responding to each type can feed into an overarching approach of reinforcing techniques for addressing pandemic emergencies, in general.

To some, historically, we have been poorly prepared to deal with the global impact of many or all of these illnesses. To others, the reality of drug resistant, emerging and re-emerging infectious disease has been a spur to action that has led to the creation of rapid response units and global detection systems. To capture a snapshot of the current picture on these matters, this contribution will address how handling biological natural hazards involving infectious disease pandemic threats are best managed through a dynamic coupling of players across a range of response levels and sectors of action.

Background and Context

Ancient African, Asian, and European pandemics provide examples that catastrophic illness has been with us for as long as we have been recording human societal development. While it is difficult to say whether or not a new pandemic will have the same enormous impact on civilization that many feel the plague of Europe did in the fourteenth century, or the 1918 avian influenza outbreak did in the early twentieth century, it is at least clear that the study of pandemic management offers an opportunity to evaluate and reflect on the current state of public health system administrative progress. Effectively responding to these threats is a complicated process that requires unusual amounts of cooperation and coordination to be successful.

As should be clear from the discussion to follow, pandemic threats require treatment from the international level to the regional, national, local, and individual ones (see chapter on ▶ "Emergency Management: International"). From global planning to local implementation, coherent and cohesive action must be closely knit together to accomplish pandemic infectious disease management. In addition, differing sectors of society concerned in this type of process must be involved in coordinated action to gain the most from such preparations. While the health sector is clearly central in such a discussion, it does not exist in a vacuum. Technological advances, as well as the contours of the legal, criminal justice, social, cultural, economic, and political sectors, also hold sway on what can and cannot be done. And, with so many infectious diseases emerging directly from the natural environment, expertise and leadership from within the ecological sector is also important to leverage when describing and explaining problems, as well as crafting policy responses.

The range of players involved in such a task spans governmental, nongovernmental, and private domains, with representatives from each needing to navigate the web of interaction in order for crisis engagement to be effective. From international policymakers to on-the-ground first responders, these actors can be involved with multiple levels of response and sectors of impact or be isolated within a particular level and sector alone. Collectively organizing their actions smoothly is one core goal of pandemic management.

A defining characteristic of pandemic threats in the twenty-first century is the impact that processes of globalization have had on the ability of pathogens to spread. Advances in the movement of people, animals, and goods have accelerated the dissemination of infectious agents. As such, the context of understanding pandemics needs to be viewed through an arc of time that encompasses improving technological innovation. Today's problems require

the reassessment of quarantine strategies, engaging emerging technologies, understanding the differences faced from rural and urban outbreaks, and many more subject areas.

Human-made events, where the goal is political destabilization and change, warrant note here as well because they highlight some important effects sought from deliberately created health calamities. These are valuable concerns to include because the results are not unique to human-made crises of this type. Natural pandemics can also give rise to significant political upheaval and security concerns. The result in both cases can be the weakening of policy and cultural bulwarks, leaving room for unrest and violence to emerge.

Understanding that these issues are often addressed within pandemic threat situations provides us with a broad overarching rationale for continually assessing our collective and ongoing effort to improve the ways that we approach these hazards. Assuring that both cases and death tallies are minimized are not the only values at stake.

Planning for Naturally Occurring Pandemic Threats

Preventing future pandemic public health emergencies, or minimizing their effects during response, requires establishing health regulations and legal rules that provide ways to clearly prepare, assess, and respond to a crisis. Such conventions enable the identification and containment of risk, as well as focused and concerted action in redressing danger. These platforms then allow for sequential planning, performance measurement, and evaluation of programs as essential aspects of managing these types of events. Training, practicing, and the organization of thought and action are essential elements in this process. Applying knowledge through an "all hazards" approach to crises creates economies of scale that allow for broad-based treatment of public health threats. This systematic application of routines makes the most of generalized information while addressing the unique concerns of certain types of outbreaks. Over time, information that is learned from on-the-ground efforts is cycled through a global system of feedback and refinement.

Infectious disease pandemic threat preparations can be examined within such conceptualizations. The ongoing concern about potential flu pandemics lends itself to displaying how accepted approaches to public health pandemic management fan out from global bodies to regional ones and then to states and localities. The cycle of information sharing is not a one-way street, however. As events occur that reinforce or add to the knowledge base, it is hoped all actors in the system will update their plans in accordance with lessons learned from throughout the system.

Illustrating policy diffusion of this nature can be quickly demonstrated through the highlighting of documents offered across different levels of the international system. For example, WHO provides a "checklist" to states, governments, and health authorities readying themselves for a possible influenza pandemic (World Health Organization 2005, 2018b). WHO addresses areas of relevance for pandemic management that spans topics from preparation, to surveillance, to case treatment, to community engagement, maintaining services, carrying out research, and finally implementation within its list categories. Other levels of response engage in similar activities. Some examples are provided below.

At the regional level, the European Union provides guidance to member states through the European Centre for Disease Prevention and Control's publications on national influenza pandemic plans that is no less thorough than those of WHO (European Centre for Disease Prevention and Control 2018). The United States Department of Health and Human Services presents a national influenza pandemic plan that serves as one model for addressing a flu-based scenario (United States Department of Health and Human Services 2017). All actors operate with a reasonably common vision that is steeped in experience from treating the illness.

Where countries and local communities are concerned, governmental and nongovernmental players are best advised to craft legal, policy, and

funding instruments that will facilitate and guide response during a pandemic emergency that make use of accepted global and regional strategies but also take note of their unique settings. A wide range of legal and regulatory scaffolding exists that can be offered as examples for exploring options. All should be coordinated as best as possible with international understandings of pandemic management. Mutual aid agreements that cut across jurisdictions and localities, as well as a variety of public-private partnerships, often are useful means of providing a unified vision for how to react to such situations at the base level of communities and local governments, where the heart of the actual work fighting disease spread will take place. To the extent these efforts dovetail with the international image for redressing infectious disease spread, so much the better.

As an example of a country-level arrangement, the United States applies a comprehensive planning approach to both human-made and natural hazards that uses a variety of frameworks designed to guide the phases of emergency management at the national level. Built to maximize the logic of the all hazards model in real-world settings, and acting in concert with the National Incident Management System (NIMS), these frameworks focus on aspects of the emergency management cycle while offering perspective to how roles and tasks may dovetail across the process. Local and state American governments are engaged in their own planning activities, as well. Pandemic emergency preparation across all levels falls within this broad conceptualization of mitigation, preparedness, response, and recovery (Lindsay 2012).

Managing Naturally Occurring Pandemic Threats

As the above documents display, planning only takes preparedness so far. Ensuring effective action in pandemic response requires that the plans be tested and appraised on a regular basis, in order that weaknesses can be identified. It also mandates that lessons can be both learned from, and integrated back into, the planning cycle. Communicating strategies, training first responders, and educating civilian populations about where to find information and resource caches become important aspects of this endeavor. Examining the effectiveness and efficiency of such activities then rests on properly constructing, analyzing, and understanding performance indicators and results in relation to intended strategies, missions, and operational goals. Plans developed and left in vacuums over time risk becoming unhelpful at best or even deadly in worst-case scenarios. Of course, central to achieving these aims is establishing a secure and operational health infrastructure that can be relied upon during an emergency. As noted below, the roles of international governmental organizations, international nongovernmental organizations, and donor states take on special importance where struggling countries are concerned.

One of the most important aspects of minimizing infectious disease pandemic threats involves active surveillance and information gathering to further prevention. This is true at all levels of identification and response. As many infectious disease pathogens are of zoonotic origin, it is clear that ongoing efforts to monitor the natural environment are imperative to the quick management and response of developing crises and could be the key to preventing a local outbreak from turning into pandemic spread. The hunting of new pathogens, as well as tracking the emergence of known ones, remains critically important in controlling public health upheavals.

While some states are better prepared to carry out these activities than others due to expertise and resource availability, those in less capable positions are equally important to carrying out the overall task at hand. As such, WHO, other relevant members of the United Nations system of international governmental organizations, supporting states, and organizations from global civil society, can be found providing personnel, skills, and guidance in these circumstances when needed.

The Global Outbreak Alert and Response Network (GOARN), in effect since 2000 and supported by the International Health Regulations (IHR) of 2005, created a WHO network of partners with the

ability to coordinate and provide the delivery of needed services to locations with health emergencies (Global Outbreak Alert and Response Network 2018). A comprehensive Events Management System is managed by WHO to further serve this purpose, and its Strategic Health Operations Centre monitors a wide range of public health issues on an ongoing basis. Addressing pandemic threat from infectious disease in relevant scenarios effectively starts with gathering the data for review at the local and country levels long before pandemic intensity is reached and then analyzing results within this international structure.

Once a new threat has been identified, response and recovery actions must be quickly engaged. Cases must be treated, and, where necessary, contacts must be traced for the work of managing spread to effectively occur. If vaccines exist, and are available, they need to be dispensed to affected populations. Best practices for controlling the particular disease must be put into effect beyond vaccine protocols as well, often modifying cultural and social norms for the benefit of enhancing safety specific to a given disease's modus operandi.

Establishing the tools to handle emergency pandemic threats needs to be connected to the awareness that rapid deployment of funds and resources may be necessary, often without a great deal of warning. This fact is consistent across sectors, actors, and levels of response. However, the degree of support required from the international system will vary based on need. In the case of WHO, establishing capacity at the global level to support states suffering outbreaks and health crises has been developed through the Contingency Fund for Emergencies (CFE). CFE was started in the wake of the 2014 Ebola outbreak in West Africa and is a part of WHO's broader Health Emergency Program. While not designed for infectious disease engagement alone, the CFE allows for rapid disbursement of financial resources to targeted recipient states that are facing extreme, and often unforeseen, health challenges. This could easily be the case where the threat of pandemic spread is involved. To the extent such financial resources can be made to affected countries and regions rapidly, worst-case pandemic scenarios stand a better chance of being avoided. This new funding structure offers WHO the ability to begin its work in crisis scenarios and settings early, as well as to support state activities as soon as possible. Other fiscal and material supports from the international system of governmental organizations, states, and civil society can take longer to mobilize (World Health Organization 2017a).

Global civil society offers additional support structures to prepare for, and respond to, pandemic threats. The Global Fund, for example, provides ways for donors to directly connect with those affected by specific health crises involving HIV/AIDS, tuberculosis, and malaria (The Global Fund 2018). It expressly recognizes that building strong health systems enables wider protection against a range of infectious diseases that are already, or could turn into, pandemic threats.

In furtherance of these goals, the organization offers supporters the ability to engage in these activities as one shot or ongoing efforts. Additionally, a variety of direct relief and support services can be found in the wealth of medically focused INGOs willing to engage health crises on the ground. Groups such as Doctors Without Borders and the International Federation of Red Cross and Red Crescent Societies are among the better known of these organizations and often find themselves in the thick of the pre-pandemic fight.

Formally recognizing the existence of a pandemic threat takes place at the highest tier of the system of response, even while a disease may be progressing on the ground in local, national, and regional settings. The fact that the disease is already active requires that the central actors recognize and categorize said threat for what it is as quickly as possible. Recognition supports the plans that have been designed for response being put into action across levels of the international system. Triggering mechanisms, such as the one described below, enable rapid and efficient coordinated response from the top down rather than sluggish and confused vertical and horizontal engagement.

At the international level, the Public Health Emergency of International Concern (PHEIC)

declaration is of critical importance to combating infectious disease spread, serving as an early warning device against possible pandemic emergence. Since the early 2000s, there has been an active effort to empower WHO, through the IHR, in a way that would invigorate response to global health dangers by encouraging concerted efforts of varied players in the political arena. Among the outcomes of this pursuit has been the creation of the PHEIC declaration that the body can pronounce in reaction to significantly threatening circumstances. Driven by WHO's IHR Emergency Committee, a committee that provides advice to the director general of the organization, declarations of this nature can be used to assuage confusion and disagreement by states, intergovernmental organizations, and international nongovernmental organizations as to the extent of a particular problem. Issuance of a PHEIC declaration signifies that the body agrees a public health threat meets the following criteria:

> i: to constitute a public health risk to other states through the international spread of disease; and
> ii: to potentially require a coordinated international response. This definition implies a situation that: is serious, unusual or unexpected; carries implications for public health beyond the affected State's national border; and may require immediate international action. (World Health Organization 2017b)

Since 2007, when the IHR on this matter came into effect and formalized the PHEIC declaration as a tool WHO could utilize, it has been used on four occasions. The first involved H1N1 in 2009, the second involved Polio resurgence in 2014, Ebola in 2014, and most recently Zika Virus in 2016. The importance of the PHEIC declaration is in the ability to develop a concerted vision of a crisis that captures competing parties and viewpoints as it welds a common position together. Indeed, the role this body of experts plays in the process speaks to how actors across levels of governance can be brought into the overall process of decision-making in a respectful, and hopefully productive, manner. As such, the process of deliberation, and the declaration itself, represents a mechanism for channeling energy and ideas – creating a critical means of linking stakeholders to each other across domains and levels of response as they craft more unified policy positions. While announcing the existence of a full-fledged pandemic will come later, if required, one value of the PHEIC declaration is in its ability to begin that process as early in the term of an outbreak as possible.

Conclusion

The best prevention, when managing biological hazards that can become pandemics, is to engage the threat as early as possible. If a threat cannot be identified or stopped in the natural environment before it appears in local human communities, then it must be pursued there. If it breaks free from these surroundings to include whole states or beyond, then it must be engaged in that wider venue. Once an infectious disease outbreak is understood to be expanding to other countries, health authorities at all levels of the system must move quickly to minimize its coverage prior to it reaching worldwide levels. The overall process is one of continuous identification and response. However, the purpose of the process does not mean the earliest alerts will be taking place when the first cases of an outbreak unfold. It does mean, however, that the alerts sounded must be made as soon as possible in the development of pandemic threats. If the earliest efforts to recognize and stop infectious disease emergence fail at the local and country levels, then international dissemination of the pathogen must be flagged for response as rapidly as possible, relying on the wealth of resources and knowledge discussed throughout this contribution.

Cross-References

► Emergency Management: International

Acknowledgments Support for this project was provided by a PSC-CUNY Award, jointly funded by The Professional Staff Congress and The City University of New York. I would like to thank Mr. Darryl Bobb, a recent graduate of John Jay College of Criminal Justice, for research assistance on the grant.

References

European Centre for Disease Prevention and Control. (2018). *Influenza pandemic preparedness*. Available at: https://ecdc.europa.eu/en/seasonal-influenza/influenza-pandemic-preparedness. 21 Oct 2018.

Global Outbreak Alert and Response Network. (2018). *Global Outbreak Alert and Response Network (GOARN)*. Available at: http://www.who.int/ihr/alert_and_response/outbreak-network/en/. 21 Oct 2018.

Lindsay, B. R. (2012). *Federal emergency management: A brief introduction*. Available at: https://fas.org/sgp/crs/homesec/R42845.pdf. 21 Oct 2018.

The Global Fund. (2018). *Focus on: Global Health Security*. Available at: https://www.theglobalfund.org/media/7318/publication_globalhealthsecurity_focuson_en.pdf. 21 Oct 2018.

United States Department of Health and Human Services. (2017). *Pandemic influenza plan: 2017 update*. Available at: https://www.hsdl.org/?abstract&did=802149. 21 Oct 2018.

World Health Organization. (2005). *Epidemic alert and response: WHO checklist for influenza pandemic planning*. Available at: http://www.who.int/csr/resources/publications/influenza/WHO_CDS_CSR_GIP_2005_4/en/. 21 Oct 2018.

World Health Organization. (2010). *What is a pandemic?* Available at: http://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/en/. 21 Oct 2018.

World Health Organization. (2017a). *Contingency fund for emergencies: Report of the WHO Health Emergencies Program/April 2017*. Available at: http://www.who.int/emergencies/funding/contingency-fund/CFE_Impact_2017.pdf. 21 Oct 2018.

World Health Organization. (2017b). *IHR procedures concerning public health emergencies of international concern (PHEIC)*. Available at: http://www.who.int/ihr/procedures/pheic/en/. 21 October 2018.

World Health Organization. (2018a). *List of blueprint priority diseases*. Available at: https://www.who.int/blueprint/priority-diseases/en/. 21 Oct 2018.

World Health Organization. (2018b). *A checklist for pandemic influenza risk and impact management: Building capacity for pandemic response -2018 update*. Available at: http://www.who.int/influenza/preparedness/pandemic/influenza_risk_management_checklist_2018/en/. 21 Oct 2018.

Further Reading

Arnold, C. (2018). *Pandemic 1918: Eyewitness accounts from the greatest medical holocaust in modern history*. Michael O'Mara Books Limited. New York: St. Martin's Press.

Garrett, L. (1994). *The coming plague: Newly emerging diseases in a world out of balance*. New York: Farrar, Straus and Giroux.

McNeill, W. (1977). *Plagues and peoples*. New York: Anchor Books.

Natural Hazards: Tornadoes

Lucia Velotti
Department of Security, Fire and Emergency Management, City University of New York (CUNY), John Jay College of Criminal Justice, New York City, NY, USA

Keywords

Natural hazard · Protective actions · Protective behavior · Risk communication

Definition

A tornado is a rotating wind funnel generated by very large thunderstorms called supercell. In case the wind changes direction, there is an opportunity for moist and cold air to combine forming a rotating funnel.

Introduction

Tornadoes can occur everywhere. In the United States, every year there are more than one thousand tornadoes (Haddow et al. 2014). In term of seasonality, tornadoes occur more frequently from March to August and primarily during the afternoon and evening "between noon and midnight" (Haddow et al. 2014, p. 44). In the United States, tornadoes occur more frequently in an area called "tornado alley" than in other regions. Tornado alley is an area covering several states such as Texas, Oklahoma, and Kansas. However, the number of tornadoes now occurring in the southeast, such as in Mississippi, Alabama, Arkansas, Missouri, and Illinois, is becoming frequent (Berardelli, December 16, 2018). The main consequences in this shift in tornado location are that damage is worse due to the dense population and number of trees in these areas that prevent people from spotting them on the ground. In addition, there are more frame houses in this region than in Oklahoma for instance, meaning that the homes are vulnerable (Berardelli, December 16, 2018).

Important aspects of tornadoes management involve damage measurement, risk communication (such as how do we warn the population about potential or actual risk), protective measures (e.g., actions people are required to undertake on the basis of their location), and people's behavior in responding to this threat. The following sections will discuss these points.

Tornado Damage Measurement and Wind Speed Estimates

The intensity and the impact of a tornado on both the built environment and vegetation are measured by the Enhanced Fujita **scale** (EF-**Scale**). The Enhanced Fujita scale, ranging from 0 to 5, has been adopted in the United States and Canada since 2007 to replace the Fujita–Pearson scale due to its limitations. The Fujita–Pearson scale (F-Scale) was developed to measure the severity of a tornado and to associate wind speeds to the level of damage. The Fujita scale measures damages from light to massive on an intensity scale of 0–5 and it is troublesome for all those cases in which the tornado does not cause any damage to the built environment. The Fujita scale is limited since it is difficult without a structural damage to classify the intensity of the tornado. In addition, the Fujita scale measures the tornado severity on the basis of the most severe structural damage without taking into account the resistance and quality of the affected building. It has to be noticed that, even though the Enhanced Fujita scale revised the wind speed of tornadoes, it still provides an estimate of wind speed and not a measurement. Table 1 shows the Enhanced Fujita scale with the associated description of damages, wind speed, and typical observation.

The deadliest tornado in the United States was the March 18, 1925, Tri-state tornado which encompassed the states of Missouri, Illinois, and Indiana. This tornado killed 695 people, of which 613 in the sole state of Illinois. The widest tornado ever recorded in the United States is the EF 5 El Reno tornado recorded on May 31, 2013, in Oklahoma with a 2.6-miles (4.2 km) width (The National Weather Service). To have an idea of the width of the tornado, it is useful to remember that 2.6 miles is the actual length of central park in New York City (Climate Central, May 4th 2013). The El Reno tornado showed the importance of taking into account possibilities rather than probabilities. Even though EF5 tornadoes are the most severe tornadoes, what really makes a difference

Natural Hazards: Tornadoes, Table 1 Enhanced Fujita scale

Scale	Damage	Wind speed	Typical observation
EF 0	Light	65–85 MPH	Peels surface off some roofs; some damage to gutters or siding; branches broken off trees; shallow-rooted trees pushed over
EF 1	Moderate	86–110 MPH	Roofs severely stripped; mobile homes overturned or badly damaged; loss of exterior doors, windows, and other glass broken
EF 2	Considerable	111–135 MPH	Roofs torn off well-constructed houses; foundations of frame homes shifted; mobile homes completely destroyed; large trees snapped or uprooted; light-object missiles generated; cars lifted off ground
EF 3	Severe	136–165	Entire stories of well-constructed houses destroyed; severe damage to large buildings such as shopping malls; trains overturned; trees debarked; heavy cars lifted off the ground and thrown; structures with weak foundations blown away some distance
EF 4	Devastating	165–200	Well-constructed houses and whole frame houses completely leveled; cars thrown; and small missiles generated
EF 5	Incredible	Over 200	Strong frame houses leveled off foundations and swept away; automobile-sized missiles fly through the air in excess of 100 m (109 yd); high-rise buildings have significant structural deformation; incredible phenomena will occur

Source: Adapted and retrieved from: Weather.com (April, 2015). The Enhanced Fujita Scale: How Tornadoes are Rated. Retrieved on February 3rd from: https://weather.com/storms/tornado/news/enhanced-fujita-scale-20130206

are the mitigation activities, the preparedness, and response of the affected communities.

Risk Communication, Tornado Watch, Tornado Warnings, and Tornado Emergency

In the United States, the National Weather Service (NWS) is the public agency responsible for issuing severe weather forecasts to the public. To this aim, the agency designed the Severe Weather Watch/Warning System. The purpose of the severe weather watch/warning system is to alert the public to hazardous weather situations and encourage them to take actions to enhance protection of life and property, despite recognizing that the final decision falls on individuals and households (Black and Ashley 2011). In order to fulfill its mission, the NWS defines both tornado watch and warning on the basis of the level of threat posed to people and to the action to be undertaken for each case (Pifer and Mogil 1978). The watches and warning are used for a variety of hazards such as floods, hurricanes, and thunderstorm and are considered as the cornerstone of severe weather risk communication. Tornado watch means that the "conditions are favorable for the development of tornadoes in and close to the watch area. During the watch, people should review tornado safety rules and be prepared to move a place of safety if threatening weather approaches" (NWS, Glossary). Tornado warning is issued by the National Weather Service when "a tornado is indicated by the WSR-88D radar or sighted by spotters" (NWS, Glossary). Under special circumstances, the NWS also issues Tornado emergencies.

A tornado emergency is a step-up to tornado warning and it is issued for all those situations that are extremely life-threatening in highly populated areas. The reason for which tornado emergency is issued in addition to tornado warning is that some communities might be accustomed and therefore complacent to tornado warnings. The first tornado emergency was issued on May 3, 1999, during the Bridge Creek EF5 outbreak and the last to date was issued during the Lee County, Alabama, March 3rd tornado, where 23 people lost their lives. Since the first tornado emergency, a total of 129 tornado emergency have been issued.

Another way to warn population of an incoming tornado threat is through the use of sirens. However, this is not always the best way. For instance, in Hodler's (1982) study of public response to the Kalamazoo Tornado, 17% of respondents did not understand the meaning of the warning siren that was sounded in order to warn citizens of potential danger, despite the fact that the sirens were tested every month. Other factors impacting people's understanding of warnings includes the amount of information conveyed through a message (DiGiovanni et al. 2002), the amount of time spent living in a specific area (Haas et al. 1977; Foster 1980; Perry and Greene 1983; Perry and Lindell 1986; Blanchard-Boehm 1998), and sociodemographic characteristics. For instance, the content of the warning can be misunderstood because of cultural or language barriers (Aguirre 1988), or because of the use of technical terms such as the use of probability to refer to the occurrence of a tornado (Morss et al. 2010) and some scholars have even suggested that terms such as watch and warning may contribute to a lack of understanding (Powell and O'Hair 2008; Donner et al. 2007).

Protective Action

The protective actions to be undertaken by people in the affected area in case of a tornado warning depend on one's location. If at home or in a business, the safest place to be according to Federal Emergency Management Agency (FEMA) are safe rooms and ICC 500 storm shelters, if either of these have been installed. Safe rooms and ICC 500 storm shelters are particularly recommended for those areas often affected by tornadoes such as those located in a "tornado alley." In absence of a safe room or ICC 500 storm shelters, the most interior windowless room located at the lower level of the house, such as a closet or a bathroom or a basement, are preferred. It is important in all of these situations to get additional protection through the use of

mattresses and blankets which serve to cover residents in order to mitigate the effects of flying debris. If in a car, the best thing to do pull off the road and try to reach safe shelters; if this is not possible, the next best option is to lie in a ditch face down with one's head covered by both hands.

However, the choice of which protective action to undertake can also be confusing for the population under warning in case of overlapping hazards. For instance, during the 2017 Hurricane Harvey in Texas, the NWS issued several overlapping tornado warning and flash flood warnings. The protective actions in case of flash flood warning (i.e., get to higher ground) are the opposite to those in case of a tornado warning, the latter of which required people at home to go to the lower level (Evans 2018).

Conclusion

In conclusion, tornadoes are a complex natural hazard which varies in intensity and therefore in loss of lives and properties. While, in the United States, there are some areas such as the tornado alley that are more tornado prone than others, even less prone states or states which usually are affected by less intense tornadoes should be ready to prepare for, heed the warning, and undertake protective actions. Particular attention should be posed at the understanding of warning terms such as tornado watch and tornado warning in conjunction with the potential existence of disaster subcultures.

Cross-References

► Emergency Management: Preparedness and Planning

References

Aguirre, B. E. (1988) The lack of warnings before the Saragosa tornado. *Int. J. Mass Emerg. Disasters, 6*, 65–74.

Berardelli, J. (2018, December 16). Tornado alley might be shifting to densely populated southeast, study shows. *CBS News*. Retrieved on 4 Feb 2019, from https://www.cbsnews.com/news/tornado-alley-may-be-moving-to-southeast-climate-change-noaa-national-severe-storms-laboratory-oklahoma-study/

Black, A. W., & Ashley, W. S. (2011). The relationship between tornadic and nontornadic convective wind fatalities and warnings. *Weather, Climate, and Society, 3*(1), 31–47.

Blanchard-Boehm, R. D. (1998) Understanding public response to increased risk from natural hazards: Application of the hazards risk communication framework. *Int. J. Mass Emerg. Disasters, 16*, 247&278.

DiGiovanni, C., B. Reynolds, R. Harwell, & Stonecipher, E. (2002). A prospective study of the reactions of residents of an American community to a bioterrorist attack. Defense Threat Reduction Agency.

Foster, H. D., (1980). *Disaster Planning: The Preservation of Life and Property*. Springer-Verlag, 255 pp.

Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2014). *Introduction to emergency management*. Butterworth-Heinemann, Kidlington Oxford UK

Climate Central. (2013, 4 June). Killer El Reno Tornado was the widest ever recorded: NWS. Retrieved on 3 Feb 2019, from https://www.climatecentral.org/blogs/killer-el-reno-tornado-was-widest-ever-recorded-nws-18308

Donner, W. R., Rodriguez, H., & Diaz, W. (2007, January). Public warning response following tornadoes in New Orleans, LA, and Springfield, MO: A sociological analysis. In *Second symposium on policy and socio-economic research, 87th annual meeting of the American Meteorological Society, San Antonio, Texas*.

Evans, J. (2018). Tornado warnings in flash flood emergencies: What do we expect people to do? *Bulletin of the American Meteorological Society, 99*(8), 1517–1518.

Haas, J., H. Cochrane, & Eddy, D. G. (1977) Consequences of a cyclone on a small city. Ekistics, 44, 45–50.

Hodler, T. W. (1982). Residents' preparedness and response to the Kalamazoo tornado. *Disasters, 6*(1), 44–49.

Morss, R., J. K. Lazo, & Demuth, J. L. (2010) Examining the use of weather forecasts in decision scenarios: Results from a US survey with implications for uncertainty communication. *Meteor. Appl., 17*, 149–162.

Perry, R. W., & Greene, M. (1983) *Citizen Response to Volcanic Eruptions: The Case of Mt. St. Helens*. Irvington Publishers, 145 pp.

Perry, R. W., & Lindell, M. (1986). *Twentieth century volcanicity at Mt. St. Helens: The routinization of life near an active volcano*. Tempe: School of Public Affairs, Arizona State University, Tech. Rep. 179 pp.

Pifer, B., & Mogil, H. M. (1978). NWS hazardous weather terminology. *Bulletin of the American Meteorological Society, 59*(12), 1583–1588.

Powell, S. W., & O'Hair, H. D. (2008). Communicating weather information to the public: People's reactions and understandings of weather information and terminology. In Preprints, *3rd symposium on policy and socioeconomic impacts*, New Orleans, LA, American Meteorological Society, Poster 1.3. http://ams.confex.com/ams/pdfpapers/132939.pdf. Accessed 7 Feb 2012.

Further Reading

Goswick, J., Macgregor, C. J., Hurst, B., Wall, P. J., & White, R. (2018). Lessons identified by the Joplin School Leadership after responding to a Catastrophic Tornado. *Journal of Contingencies and Crisis Management, 26*(4), 544–553.

Schumann, R. L., III, Ash, K. D., & Bowser, G. C. (2018). Tornado warning perception and response: Integrating the roles of visual design, demographics, and hazard experience. *Risk Analysis, 38*(2), 311–332.

This tornado was particularly remarkable not only because of its width, but also because storms do not usually travel from west to east.

Natural Hazards: Tsunamis

Lucia Velotti
Department of Security, Fire and Emergency Management, City University of New York (CUNY), John Jay College of Criminal Justice, New York City, NY, USA

Keywords

Vertical evacuation · Tsunami · Natural hazards · Hazard mitigation

Definition

A tsunami is a "big wave" or a series of waves that can be triggered by earthquakes, landslides, mudslides, and volcano explosions (Godschalk 2007; Haddow et al. 2013; Mileti 1999).

Introduction

A tsunami, or "big wave," can be triggered by an earthquake, landslide or mudslide (Godschalk 2007; Haddow et al. 2013; Mileti 1999), and volcano explosions. An example of a tsunami generated by landslide is the 1963 Vajont dike tsunami in Italy. The 820 feet high wave was generated by a landslide into the lake which then overtopped the dike. The wave submerged several villages in the valley leaving 1905 people dead. Tsunami can also be triggered by volcanoes. Examples of tsunami generated by volcano can be those generated by the Stromboli, in Italy, in 1919, 1956, and 1930.

Nowadays, the kind (type) of tsunami best known by the general public is the tsunami triggered by earthquake such as the 2004 Indian Ocean tsunami and the 2011 Japanese Tohoku earthquake/tsunami. Unlike other hazards, such as hurricanes, tornadoes, and earthquakes, tsunamis do not have a scale to measure their intensity or their ability to create damages. However, when triggered by an earthquake, tsunamis can be classified as near-source, medium-source, and far-source-generated (Godschalk 2007; Haddow et al. 2013). The nearer the source that generates the tsunamis, the lesser the time available for people to undertake a protective behavior such as evacuating to higher ground or further inland. For instance, a near-source-generated tsunami would leave people anywhere from 5 to 20 min to undertake protective action, while a far-source-generated tsunami could leave up to 6 or more hours to reach the shore. A tsunami hazard is also a complex hazard to plan for. Complexities in planning for tsunamis are due to the presence of two hazards, the earthquake and the tsunami, and the interaction of these hazards with the human settlement or hazardous sites and other hazards such as landslides. Tsunamis can be deadly and expensive. For instance, the March 2011 Tohoku earthquake (Japan) caused the death of 15,891 people (Oskin 2015) and an estimated 309 billion dollars in property damages. However, the deadliest earthquake/tsunami, in recent times, was the 2004 Indian Ocean tsunami with a death toll of approximately 300,000 (Fritz et al. 2006).

The threat of tsunami in the United States is concentrated in the West Coast of the country, particularly in the coastal areas of Alaska, Oregon, Washington, and part of California as a consequence of the Cascadia subduction zone (CSZ). The East Coast of the United States can also be at risk of tsunami (Seismological Society of America, April 19, 2013).

The last CSZ earthquake-triggered tsunami occurred in 1700. This event is comparable to the 2011 magnitude 9.0 (Richter scale) Japanese Tohoku earthquake and tsunami and the February 27, 2010M 8.8 earthquake and tsunami in Maule,

Chile (CREW 2013). The chance of a magnitude 9.0 (Richter scale) earthquake occurring along the CSZ within the next 50 years is 10% (CREW 2013). Further, a tsunami triggered by an earthquake in the CSZ will give the inhabitants of the proximate coastal areas a lead time of between 15 and 30 min to look for safety. Different means of overcoming the threat are being contemplated based on the estimated arrival time of the tsunami wave, proximity to high ground, and population demographics. In the United States, it is assumed that people in areas with a nearby high ground will easily reach safety by going to high ground, reaching at least 100 feet of elevation, or going 1 mile inland (FEMA, March 18, 2013). Going to higher ground might be particularly challenging or people to gain safety by reaching higher ground, the fact that not everyone will be able to reach higher ground in time. This is particularly true in the case of vulnerable populations such as the elderly, people with reduced mobility, and tourists who might be unaware of the surrounding area. In addition, time to reach safety is calculated at the individual level, rather than the time it takes to evacuate in groups, as is the case for evacuating families (Velotti et al. 2013). Thus, in preparing communities for tsunami emergency, managers and public planners face several challenges.

Tsunami Hazard Mitigation Measures

Hazard mitigation by definition is made up of two main goals: reducing and minimizing loss of property and reducing and minimizing loss of lives. A general classification of hazard mitigation measures is based on the presence of engineering intervention in structural or nonstructural measures (Rossi et al. 1982; Tierney 1989). Structural measures rely on the use of engineered interventions to reduce the impact of a hazard, while nonstructural measures do not. A more thorough description of mitigation measures provided by FEMA associates hazard mitigation goals to mitigation strategies. FEMA identifies five main mitigation goals: (1) property protection, (2) prevention, (3) public education and awareness, (4) critical facilities protection, and (5) structural projects. Each of the mitigation goals and related mitigation strategies are described below. While these are general mitigation measures, the examples used will refer to tsunami hazards.

Prevention measures are aimed at minimizing the impact of a tsunami in terms of loss of life, primarily by reducing the density of occupancy in tsunami inundation zones, especially for tsunami run-up areas. Prevention measures mainly refer to land use management such as open land development regulations, planning and zoning, and open space preservation. For example, open space preservation refers to the maintenance or to the conversion of specific at-risk areas to parks or agriculture land.

Property protection measures such as acquisition, relocation, and rebuilding can also be used as mitigation measures in order to protect critical facilities (e.g., hospitals, emergency operation centers [EOC], schools, and so on). Property protection measures are very effective (Berke and Beatley 1992), but they are also among the most expensive mitigation strategies (Rossi et al. 1982). Acquisition relates to the purchase of a building or an area that is considered under threat, usually by a public entity. Once the site is purchased, it is no longer possible to build anything on it. Acquisition is generally followed by relocation and therefore rebuilding. For example, if a school lies in a flood or tsunami inundation area, the land on which the school is built can be acquired and the school relocated and rebuilt in a safer area.

Public education and awareness include those activities aimed at improving the chances of survival and people's self-reliance in an attempt to lessen their vulnerability and keep hazard awareness high. Mitigation actions that can be undertaken in this category are the production of maps, indicating the tsunami inundation zone and the safest place where to evacuate, and public outreach activities informing different target categories of people/organizations of risks and protective actions. Examples of public education as a mitigation measure are the attempts to create a new disaster subculture (Velotti et al. 2013) and educating people to self-assess the danger and take action. The creation of a new disaster

subculture in the case of tsunami relies on the Japanese concept of Tendenko, meaning "each for themselves" (Yamori 2014). Tendenko teaches people mutual trust in the fact that everybody will attempt to gain safety; this approach saved many lives during the 2011 Tohoku earthquake/tsunami. Education proved to be meaningful in saving the lives of Japanese school children at Unosumai, Kamaishi City, where the children were able to self-assess the safest location on the basis of the wave height and evacuated uphill rather than to the third floor of their school (Fraser et al. 2012; Harding and Harding 2011; Hein 2014; Yamori 2014).

Natural resources protection in case of tsunamis is aimed at preserving the natural landscape as a way to slow the tsunami forces. For instance, in the aftermath of the 2004 Indian Ocean tsunami, there has been greater advocacy for the restoration of mangroves along the beaches as a mitigation measure.

Structural projects involve the use of engineered structures such as seawalls, dams, vertical structures, and so on. The protective ability of structural projects is limited by the provision of safety up to a preplanned threshold (Berke and Campanella 2006; Burby et al. 2000; Burby 2006; Burby and Dalton 1994; Clary 1985; Highfield and Brody 2006; Mileti 1999; Rossi et al. 1982). For instance, a dam or a seawall can be designed to withstand a predetermined impact, but once that threshold is passed, the structural integrity of the dam or seawall can no longer be guaranteed. Thus, structural projects could result in the "safe development paradox" (Burby 2006). For instance, the government's authorization to develop an area that is at risk could have an unintended consequence in the event of structural protection failure. For example, people might feel safe that they are being protected by a dam and do not undertake any other mitigation measure.

Tsunami Protective Actions

Vertical evacuation (VE) has been adopted, implemented, and tested as a protective strategy in Japan to handle tsunami and in Bangladesh to handle recurrent hazards such as cyclones (Nirupama 2013). Attempts to implement VE are also being made in some of the countries affected by the December 26, 2004, Indian Ocean tsunami (GeoHazards International 2014). Examples of vertical shelters built for VE are the Nishiki tower and the Tasukaru (life-saving) tower. The Nishiki tower is a multi-purpose building used as the mayor's office and a tsunami museum to promote awareness. It has a capacity to hold approximately 500 people, has a height of 71.5 feet, and has a sheltering area starting at an elevation of 66.2 feet (Nakaseko et al. 2008). In addition to the Nishiki tower, 16 other shelters were built between 1994 and 2005. The Nishiki tower also serves the mitigation goal of educating and making people aware of the tsunami threat.

These buildings are the starting point for discussions on the adoption of vertical shelters or tsunami VE building (Fraser et al. 2012) and VE in the United States in the States of Washington and Oregon. Nowadays, the first vertical evacuation shelter in the United States has been built at the Ocosta School in the State of Washington.

Conclusion

In conclusion, a tsunami triggered by earthquake is a complex hazard to be planned for because of the many variables and uncertainties involved. In the mitigation stage, the best measure could be not allowing people to live in at-risk areas; however, this is not always the best solution since people are resistant to resettlement and moving communities is expensive. Vertical evacuation shelters seem to be a viable solution to help those who will not be able to reach high ground on time and eventually also the most vulnerable population such as the elderly and the people with impairment, for instance. Resistance toward the building of vertical shelters in the United States is due to the fact that these shelters are not safe but are the safer option in some specific cases. Government representatives are afraid of being liable for loss of lives in case the shelter is overtopped by a tsunami wave.

Cross-References

- ▶ Fire: Evacuation (Engineer Solutions)
- ▶ Natural Hazards

References

Berke, P. R., & Beatley, T. (1992). *Planning for earthquakes: Risks, politics, and policy*. Baltimore: John Hopkins University Press.

Berke, P. R., & Campanella, T. J. (2006). Planning for post-disaster resiliency. *Annals of the American Academy of Political and Social Science, 604*(1), 192–207.

Burby, R. (2006). Hurricane Katrina and the paradoxes of government disaster policy: Bringing about wise governmental decisions for hazardous areas. *The Annals of the American Academy of Political and Social Science, 604*(3), 171–191.

Burby, R. J., & Dalton, L. C. (1994). Plans can matter! The role of land use plans and state planning mandates in limiting the development of hazardous areas. *Public Administration Review, 54*, 229–238.

Burby, R. J. and May, P. J. (1997). *Making governments plan: State experiments in managing land use*, Johns Hopkins Uniiversity Press, Baltimore.

Burby, R. J., Deyle, R. E., Godschalk, D. R., & Olshansky, R. B. (2000). Creating hazard resilient communities through land-use planning. *Natural Hazards Review, 1*(2), 99–106.

Cascadia Region Earthquake Workgroup (CREW). (2013). Cascadia subduction zone earthquakes: A magnitude 9.0 earthquake scenario. Retrieved on September 1, 2014 from: http://crew.org/sites/default/files/cascadia_subduction_scenario_2013.pdf

Clary, B. B. (1985). The evolution and structure of natural hazard policies. *Public Administration Review, 45*, 20–28.

Fraser, S., Leonard, G. S., Matsuo, I., & Murakami, H. (2012). Tsunami evacuation: Lessons from the Great East Japan earthquake and tsunami of March 11th 2011. GNS Science Report 2012/17, p. 89.

Fritz, H. M., Synolakis, C. E., & McAdoo, B. G. (2006). Maldives field survey after the December 2004 Indian Ocean tsunami. *Earthquake Spectra, 22*(S3), 137–154.

Godschalk, D. R. (2007). Mitigation. In W. L. Waugh & K. J. Tierney (Eds.), *Emergency management: Principles and practice for local government*. Washington, DC: International City/County Management Association.

Geohazards International. (2014). Tsunami preparedness–feasibility study of vertical evacuation structures in Sumatra. Available via http://geohaz.org/projects/sumatra.html. Accessed February 5, 2019.

Haddow, G., Bullock, J., & Coppola, D. P. (2013). *Introduction to emergency management*. Butterworth-Heinemann, Massachusetts.

Harding, D., & Harding, B. (2011). Tendenko: Surviving the Tsunami. Al Jazeera.

Hein, P. (2014). Expecting the unexpected: A case study on tsunami mitigation in Fujisawa (Japan). *Environmental Hazards, 13*(1), 1–20.

Highfield, W. E., & Brody, S. D. (2006). Price of permits: Measuring the economic impacts of wetland development on flood damages in Florida. *Natural Hazards Review, 7*(3), 123–130.

Mileti, D. (1999). *Disasters by design: A reassessment of natural hazards in the United States*. Washington D.C. Joseph Henry Press.

Nakaseko, T., Kimata, F., Tanaka, S., & Takahashi, M. (2008). Tsunami and Evacuation System in Nishiki of Central Japan. International Conference on Tsunami Warning (ICTW) Bali, Indonesia, November 12–14, 2008. Retrieved on August 1, 2011 from: http://www.seis.nagoya-u.ac.jp/kimata/ref/ICTW08_paper_CPM13JP.pdf

Nirupama, N. (2013). Vertical evacuation during cyclones: Suitable for developing countries. *Natural Hazards, 69*(1), 1137–1142.

Oskin, B. (2015, May 7). Japan earthquake & tsunami of 2011: Facts and information. Retrieved on June 18, 2015 from: http://www.livescience.com/39110-japan-2011-earthquake-tsunami-facts.html

Rossi, P. H., & Wright, J. D., Weber-Burdin, E. (1982). Natural hazards and public choice: the state and local politics of hazard mitigation. New York: Academic Press.

Tierney, K. J. (1989). Improving theory and research on hazard mitigation: Political economy and organizational perspectives. *International Journal of Mass Emergencies and Disasters, 7*(3), 367–396.

Velotti, L., Trainor, J. E., Engel, K., Torres, M., & Myamoto, T. (2013). Beyond vertical evacuation: Research considerations for a comprehensive "vertical protection strategy". *International Journal of Mass Emergencies & Disasters, 31*(1), 60–77.

Yamori, K. (2014). Revisiting the concept of tsunami tendenko: Tsunami evacuation behavior in the Great East Japan Earthquake. In *Studies on the 2011 off the Pacific Coast of Tohoku Earthquake* (pp. 49–63). Tokyo: Springer.

Further Reading

Blake, D., Johnston, D., Leonard, G., McLaren, L., & Becker, J. (2018). A citizen science initiative to understand community response to the Kaikōura earthquake and tsunami warning in Petone and Eastbourne, Wellington, Aotearoa/New Zealand. *Bulletin of the Seismological Society of America, 108*(3), 1807–1817. https://doi.org/10.1785/0120170292

Johnston, D., Paton, D., Crawford, G. L., Ronan, K., Houghton, B., & Bürgelt, P. (2005). Measuring tsunami preparedness in coastal Washington, United States. *Natural Hazards, 35*(1), 173–184.

Naylor, A., Walker, J. F., & Suppasri, A. (2018). Suitability of the early warning systems and temporary housing for the elderly population in the immediacy and transitional recovery phase of the 2011 Great East Japan Earthquake and Tsunami. *International Journal of Disaster Risk Reduction, 31*, 302–310.

Natural Hazards: Volcanic Eruptions

Hung-Lung Wei
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, CUNY, New York, NY, USA

Keywords
Ash · Earthquakes · Evacuation · Lava · Magma · Silicosis · Tephra

Definition

Volcanic eruptions refer to the types of activity, such as discharge of steam and other gases, lava, and gas-laden debris, which lead to a variety of associated problems (e.g., landslides, fires, property destruction).

Introduction

There are different types of volcanoes in terms of size and morphology. Siebert et al. (2015) indicated that "Volcanic landforms vary widely in size and morphology from the stereotypical towering glacier-clad stratovolcano. They range from small spatter cones to massive shield volcanoes several thousand cubic kilometers in volume or broad volcanic depressions, cinder cones being the most common volcanic construct. Their eruptions likewise span many orders of magnitude in volume" (p. 239).

Volcanic activity (e.g., explosive eruptions, pyroclastic flows, lava flows, lahars, ash fall, gases, acid rain, etc.) can cause a number of casualties and economic losses worldwide. For instance, Witham (2005) discovered that 491 volcanic eruptions in the twentieth century produced massive impacts on mortality, morbidity, homelessness, economic collapse, and destruction of both the human-built and natural environments. In order to protect people's lives and their property from damage, it is important to understand scientific research on volcanic eruptions, mitigation strategies, and preparedness strategies for volcanic eruptions.

Research on Volcanic Eruptions

The importance of volcano research is underscored by many international scholars who have examined volcanic risk perception or the extent of hazard adjustment adoption or both (Barberi et al. 2008; Carlino et al. 2008; Finnis et al. 2010; Gaillard 2008; Gavilanes-Ruiz et al. 2009; Haynes et al. 2008; Jóhannesdóttir and Gísladóttir 2010; Paton et al. 2008; Perry and Lindell 2008; Sagala et al. 2009; Wei and Lindell 2017). In addition, other researchers have studied volcanic risk communication (Barberi et al. 2008; Bird et al. 2009; Carlino et al. 2008; Haynes et al. 2008; Wei and Lindell 2017) and evacuation (Barberi et al. 2008; Bird et al. 2009; Carlino et al. 2008; Chenet et al. 2014; Jóhannesdóttir and Gísladóttir 2010; Marrero et al. 2013; Mei et al. 2013; Wei and Lindell 2017; Woo 2008).

In a recent volcano study of Mt. Rainier (which has not erupted since 1894), Wei and Lindell (2017) reported the average risk perception of respondents was relatively low ($M = 2.4$, based on a 5 point scale). Peacock et al. (2005) suggested that increasing public participation and people's psychological reactions to their hazard exposure are significant factors that can influence the content of hazard mitigation programs and, thus, allow people to prepare for and respond to environmental hazards. In addition, people's risk perceptions are likely to have an effect on community hazard adjustments such as emergency preparedness programs, building codes, and land use planning policies. Therefore, local and state governmental officials need to devise strategies that can improve the accuracy of people's risk perceptions in order to allow them to prepare for and respond to disaster threats appropriately. Wei and Lindell (2017) mentioned that risk communication strategies should address message content by describing the personal consequences of hazard impact and should provide repeated messages in order to increase the frequency of thought and discussion about the

hazard. Risk communication programs that are designed in this way to produce affective reactions and appropriate hazard adjustments commiserated with risk level. Moreover, Wei and Lindell (2017) concluded that most respondents had low levels of hazard intrusiveness (i.e., blending of information due to people thinking and discussing hazard-relevant information with family members or peers), resulting in very few of them to engage in volcano-specific emergency preparedness actions; consequently, local emergency managers must find effective ways to increase residents' volcano hazard awareness and preparedness to reduce potential harm from residents' poor planning in response to volcano eruptions.

Mitigation and Preparedness Strategies for Volcanic Eruptions

Lindell et al. (2006) described four mitigation measures (i.e., community protection works, land use practices, building construction practices, and building contents protection) that are suitable for volcanic eruptions. Andreastuti et al. (2018) noted that an effective disaster mitigation plan should incorporate culture and local resources and implement it through a best mitigation education program. This education program must provide the early warning system and evacuation model for the area where the community is located, allowing the community members to understand how to take protective actions such as evacuation. Also, Andreastuti et al. (2018) emphasized that effective community's responses to volcanic eruption rely on close coordination and collaboration between government and community.

Risk communication strategies can protect people's lives from volcanic eruptions. Stone et al. (2014) discussed a network of volunteers known as vigías (a community-based volcano monitoring) and discovered the vigías network functions simultaneously as: (a) a source of observational data for scientists; (b) a communication channel for increasing community awareness, understanding of hazard processes, and enhancing preparedness; and (c) an early warning system for civil protection. In a recent study of risk communication films, Hicks et al. (2017) demonstrated that risk communication is most effective when approaches are integrated into risk reduction strategies and/or research projects from the outset, and the audiences are identified, their needs are known, and they are motivated to participate in the risk communication process itself. Furthermore, communicating risk across hazard contexts and settings can support the management and reduction of risk and strengthen resilience of communities to disasters (Hicks et al. 2017).

Conducting vulnerability assessment is an important strategy for volcanic eruptions because it helps local officials and emergency managers understand and communicate where potential loss of life may be concentrated and where to focus on risk reduction efforts (Diefenbach et al. 2015). Local government agencies can apply Geographic Information System (GIS) tools to map risk areas and locations of critical infrastructure (e.g., telecommunication networks, natural gas networks, electric grids, key transportation routes, schools, hospitals, etc.) and determine values of buildings and residents that will be affected by volcanic hazards.

In a study of ash fall preparedness, Wilson et al. (2014) described a collaborative process used to create a suite of ten posters designed to improve the resilience of critical infrastructure organizations to volcanic ash fall hazards. This collaborative process attempted to create a partnership between critical infrastructure managers, other relevant government agencies along with volcanic impact scientists, and eventually translate volcanic impact research into practical management tools.

Conclusion

In the United States, local and state Departments of Emergency Management should collaborate with the USGS Volcano Hazards Program to disseminate volcanic risk maps to residents and conduct social vulnerability analysis to identify the vulnerable populations with regard to the volcanic threats (e.g., pyroclastic flows, lava flows, lahars, ash fall, gases, acid rain, etc.). It is important to increase the awareness of community

preparedness, and it can be achieved in several ways. For example, educating the children in public schools (K-12) could be efficient and beneficial because it allows them to discuss the early warning system and evacuation plan with their parents. Community organizations can be trained to play an important role in instructing people about the early warning system and evacuation plan. Finally, local emergency managers should arrange meetings for explaining the evacuation plan and provide incentives for promoting public participation.

Cross-References

- ▶ Emergency Management: Crisis Communication
- ▶ Emergency Management: Preparedness and Planning
- ▶ Federal Emergency Management Agency
- ▶ Natural Hazards

References

Andreastuti, S., Paripurno, E., Gunawan, H., Budianto, A., Syahbana, D., & Pallister, J. (2018). Character of community response to volcanic crises at Sinabung and Kelud volcanoes. *Journal of Volcanology and Geothermal Research*. (In Press).

Barberi, F., Davis, M. S., Isaia, R., Nave, R., & Ricci, T. (2008). Volcanic risk perception in the Vesuvius population. *Journal of Volcanology and Geothermal Research, 172*, 244–258.

Bird, D. K., Gisladottir, G., & Dominey-Howes, D. (2009). Resident perception of volcanic hazards and evacuation procedures. *Natural Hazards and Earth System Sciences, 9*, 251–266.

Carlino, S., Somma, R., & Mayberry, G. C. (2008). Volcanic risk perception of young people in the urban areas of Vesuvius: Comparisons with other volcanic areas and implications for emergency management. *Journal of Volcanology and Geothermal Research, 172*, 229–243.

Chenet, M., Grancher, D., & Redon, M. (2014). Main issues of an evacuation in case of volcanic crisis: Social stakes in Guadeloupe (Lesser Antilles Arc). *Natural Hazards, 73*, 2127–2147.

Diefenbach, A. K., Wood, N. J., & Ewert, J. W. (2015). Variations in community exposure to lahar hazards from multiple volcanoes in Washington State (USA). *Journal of Applied Volcanology, 4*, 4.

Finnis, K. K., Johnston, D. M., Ronan, K. R., & White, J. D. (2010). Hazard perceptions and preparedness of Taranaki youth. *Disaster Prevention and Management: An International Journal, 19*, 175–184.

Gaillard, J.-C. (2008). Alternative paradigms of volcanic risk perception: The case of Mt. Pinatubo in the Philippines. *Journal of Volcanology and Geothermal Research, 172*, 315–328.

Gavilanes-Ruiz, J. C., Cuevas-Muñiz, A., Varley, N., Gwynne, G., Stevenson, J., Saucedo-Girón, R., Pérez-Pérez, A., Aboukhalil, M., & Cortés-Cortés, A. (2009). Exploring the factors that influence the perception of risk: The case of Volcán de Colima, Mexico. *Journal of Volcanology and Geothermal Research, 186*, 238–252.

Haynes, K., Barclay, J., & Pidgeon, N. (2008). Whose reality counts? Factors affecting the perception of volcanic risk. *Journal of Volcanology and Geothermal Research, 172*, 259–272.

Hicks, A., Armijos, M. T., Barclay, J., Stone, J., Robertson, R., & Cortés, G. P. (2017). Risk communication films: Process, product and potential for improving preparedness and behaviour change. *International Journal of Disaster Risk Reduction, 23*, 138–151.

Jóhannesdóttir, G., & Gísladóttir, G. (2010). People living under threat of volcanic hazard in southern Iceland: Vulnerability and risk perception. *Natural Hazards and Earth System Sciences, 10*, 407–420.

Lindell, M. K., Prater, C. S., & Perry, R. W. (2006). *Fundamentals of emergency management*. Emmitsburg: FEMA Emergency Management Institute.

Marrero, J. M., García, A., Llinares, A., Cruz-Reyna, S. D., Ramos, S., & Ortiz, R. (2013). Virtual tools for volcanic crisis management, and evacuation decision support: Applications to El Chichón volcano (Chiapas, Mexico). *Natural Hazards, 68*, 955–980.

Mei, et al. (2013). Lessons learned from the 2010 evacuations at Merapi volcano. *Journal of Volcanology and Geothermal Research, 261*, 348–365.

Paton, D., Smith, L., Daly, M., & Johnston, D. (2008). Risk perception and volcanic hazard mitigation: Individual and social perspectives. *Journal of Volcanology and Geothermal Research, 172*, 179–188.

Peacock, W. G., Brody, S. D., & Highfield, W. (2005). Hurricane risk perceptions among Florida's single family homeowners. *Landscape and Urban Planning, 73*, 120–135.

Perry, R. W., & Lindell, M. K. (2008). Volcanic risk perception and adjustment in a multi-hazard environment. *Journal of Volcanology and Geothermal Research, 172*, 170–178.

Sagala, S., Okada, N., & Paton, D. (2009). Predictors of intention to prepare for volcanic risks in Mt. Merapi, Indonesia. *Journal of Pacific Rim Psychology, 3*, 47–54.

Siebert, L., Cottrell, E., Venzke, E., & Andrews, B. (2015). Earth's volcanoes and their eruptions: An overview. In *The encyclopedia of volcanoes* (2nd edn, pp. 239–255). Academic Press: San Diego, CA.

Stone, J., Barclay, J., Simmons, P., Cole, P. D., Loughlin, S. C., Ramón, P., & Mothes, P. (2014). Risk reduction

through community-based monitoring: The vigías of Tungurahua, Ecuador. *Journal of Applied Volcanology, 3*, 11.

Wei, H.-L., & Lindell, M. (2017). Washington households' expected responses to lahar threat from Mt. Rainier. *International Journal of Disaster Risk Reduction, 22*, 77–94.

Wilson, T. M., Stewart, C., Wardman, J. B., Wilson, G., Johnston, D. M., Hill, D., Hampton, S. J., Villemure, M., McBride, S., Leonard, G., Daly, M., Deligne, N., & Roberts, L. (2014). Volcanic ashfall preparedness poster series: A collaborative process for reducing the vulnerability of critical infrastructure. *Journal of Applied Volcanology, 3*, 10.

Witham, C. S. (2005). Volcanic disasters and incidents. *Journal of Volcanology and Geothermal Research, 148*, 191–233.

Woo, G. (2008). Probabilistic criteria for volcano evacuation decisions. *Natural Hazards, 45*, 87–97.

Further Reading

Doyle, E., McClure, J., Johnston, D., & Paton, D. (2014). Communicating likelihoods and probabilities in forecasts of volcanic eruptions. *Journal of Volcanology and Geothermal Research, 272*, 1–15.

Pyle, D. M. (2015). Sizes of volcanic eruptions. In *The encyclopedia of volcanoes* (2nd edn, pp. 257–264). Academic Press: San Diego, CA.

Rougier, J., Sparks, S., Cashman, K., & Brown, S. (2018). The global magnitude-frequency relationship for large explosive volcanic eruptions. *Earth and Planetary Science Letters, 482*, 621–629. https://doi.org/10.1016/j.epsl.2017.11.015.

P

Personnel Security: Hiring

Thomas Shea
Police Graduate Studies Program, College of Education and Human Services, South Orange, NJ, USA

Keywords
Private security · Physical security · Background investigations

Definition

Since the unfortunate events of September 11, 2001, there exists a newfound and prevalent dependency on private security in the United States. Government officials do not protect the majority of private infrastructure in this country, but rather, private security officers. An effective private security position is one that requires trust and integrity, as well as a sense of professionalism. The hiring of incompetent personnel can result in litigation, loss of revenue, and personal harm to both employees and clients in organizations. There are multiple layers of security-oriented vetting, but the preemployment hiring process is crucial to meeting objectives while safeguarding organizational assets. The likelihood of the unsuccessful hiring of an employee is usually correlational to the extent of background investigations conducted before employment.

Introduction

"Personnel security," as defined by Ortmeier and Johnson (2017), "involves protection of people associated with the organization as well as protection from those who might harm the organization or its people (p. 98)." Individuals selected for employment as personnel security officers are often granted access to sensitive information and secure physical facilities not normally accessible to the public. Unlike policing, where the objectives are to detect and apprehend criminals, the goal of security personnel is more to deter and prevent criminal activity in the first place (Blackstone and Hakim 2010). Also, there are many functions that do not require the advanced training or authority of sworn police officers. The expectation by employers and managers is that security personnel will be trustworthy and loyal to their respective organizations (Center for Development of Security Excellence-Personnel Security 2017).

According to the Bureau of Labor Statistics and as of May 2018, there were 1,114,380 security guards employed in the United States, the majority geographically located in the Northeastern United States (Bureau of Labor Statistics 2018). The majority of those individuals' work in general investigative and security job descriptions, though other descriptions included schools, hospitals, banks, and establishments that serve alcohol. There is a greater reliance on private security in many nations with respect to crime prevention and

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

detection, than solely having policing strategies in place (Johnston and Shearing 2003; Stenning 2000). In fact, it is estimated that there are twice as many private security personnel than police officers (UN News 2011). There are multiple needs and uses for private security, ranging across many infrastructural and occupational functions. The American Society of Industrial Security or ASIS (https://www.asisonline.org/), one of the world's largest and one of the most reputable security organizations in the world, listed 18 security functions, including, but not limited to:

> . . .physical security, personnel security, information systems security, investigations, loss prevention, risk management, legal aspects, emergency/continuity planning, fire protection, crisis management, disaster management, counterterrorism, competitive intelligence, executive protection, workplace violence, general crime prevention, Crime Prevention Through Environmental Design (CPTED), and security architecture. (2001)

Trends indicate that private security is the primary means of protection in the United States (Cunningham and Strauchs 1992) and worldwide (Bayley and Shearing 2001). Secondly, the profession consistently grows every year (Bureau of Labor Statistics (BLS) 2010; Behar 1992). Many commercial airports in the United States employ private security instead of TSA agents (Nixon 2016). With this many individuals employed in the myriad locations described, the chances for citizens to engage in contact of some form with security guards are high (Cunningham and Strauchs 1992). Professionalism displayed by security personnel during these interactions is of the utmost importance to create legitimacy for the organization.

According to a study by Nalla and Crichlow (2017), there is no standard protocol for the training of newly hired guards and some do not even require minimum educational standards or criminal background checks. Guards themselves also admit that the lack of training received hinder the ability to perform their jobs effectively (Cobbina et al. 2013). The creation of an accredited program for security guards has the propensity to improve the overall standards of the profession (Adolf 2011) but, so far, that has not occurred. This oversight has an inclination to increase liability for the respective, aforementioned organizations, and affect the morale of personnel security staff.

With the existing lack of consistent and reputable hiring standards, the possibilities of incidences occurring that can create liabilities increases as well. Hiring qualified security personnel is the most critical aspect of building a respected and effective security paradigm (McAdams 2004). Secondly, the complete legitimacy of the private security occupation is linked to the level of professionalism shown by employees (Nalla and Hwang 2006). Selection of the most qualified individuals available is integral to accomplish those lofty goals.

The First Step: The Background Check

A thorough, comprehensive background screening investigation must be performed on all applicants to avoid hiring an individual not qualified or who might have a criminal background. Prospective employees should be comprehensively checked to avoid missing troubling determinants in their pasts. The detection of past infractions does not usually prove to be difficult (Power and Forte 2006); however, without a unified database that screeners can utilize to retrieve background information, an incomplete investigation may be the result (Brody 2010). This concern is legitimate; however, it can be mitigated with a proficient investigator. Past reforms in personnel security clearance improved the speed and efficiency of investigations, yet those improvements remain debated by professionals and experts (Miles 2012). At a minimum, inclusion and examination of the following records should be a part of a background investigation (Fay 2011; Russell and Arlow 2015):

- State, local, national police
- Former employees
- Public records
- Credit agencies
- Schools at all levels
- References *not* furnished by applicants

Other preemployment techniques are also effective, such as "honesty," or "integrity" tests. During both tests are asked questions based on scenarios where applicants have to make ethical decisions. An example of this might include the decision whether to report a fellow employee that the applicant witnessed committing theft. Certain companies do not like to utilize these tests because some employees consider such questions offensive and an invasion of privacy (Sackett and Harris 1984). Yet, a home improvement store chain initiated an integrity test as part of their hiring process that resulted in a 50% reduction of employee terminations for theft, drug use, and violence (5 year period) (Brown et al. 1987). Terminations of employees due to misconduct create unnecessary turnover, time, and cost for the organization. Terminations for these reasons can be averted by conducting strict due diligence (Gregory 2015), therefore it should be a priority during an initial hiring process.

According to Sissons (2002), there are pragmatic vetting techniques that organizations can adopt to achieve thorough and comprehensive preemployment screening, including: (a) an explanation of the particular position so that they understand that it is more involved than infrastructure protection and also requires discretion, (b) ensuring that the applicant has verified first aid training, (c) the use of fair and adequate assessment tools, and (d) if employing applicants from an outside vendor, check the references of that company and not just the applicant. Many companies choose to employ contract security over in-house personnel because of the flexibility and cost benefits (Button and George 2005). Whether choosing to employ outsourced security personnel or not, the company is obliged to assure training and needs requirements are met (Papi 1994; Rosenberg 2007). Some organizations choose to train contracted staff in house, while others delegate that responsibility to the security vendor. With either choice, however, the hiring organizations are still liable for the acts of security personnel.

Sennewald (2011) outlines more intrinsic values that an organization should examine in security personnel candidates, such as: (a) the need to be free from mental or physical disorders that would affect performance standards; (b) demonstration of maturity, integrity, and responsibility; and (c) the absence of criminal convictions involving "moral turpitude" (p. 61). However, the promulgation of a screening process that evaluates ethical and moral values may be difficult due to its subjective nature. The combination of empirical measurement tools coupled with personnel trait assessments may develop a more complete screening instrument for employers. Even so, the evaluator must also be trained in human resources techniques to ensure correct vetting procedure implementation.

Upon hiring, employers should advise applicants that they will be monitored during the course of their daily duties. Applicants should also be notified that they must accept all mandated conditions upon acceptance of the position (Mitrou and Karyda 2006). Examples of these conditions include drug testing, credit checks, and social media checks, among others. Furthermore, employers have the incumbent responsibility to confirm that all prospective staff understand and are trained to adhere with the policies and regulations of the organization (Lincke 2015). Should a future incident occur that causes a potential litigious situation, there is a tendency for attorneys from both sides to seek this information as evidence to prove their case. There is no quicker practice to lose civil lawsuits than maintaining failure to train liabilities within an organization. Prudent safeguarding regarding personnel practices is recommended to reducing this exposure (Meadows 1987).

Negligent Hiring

There are consequences for not performing competent due diligence on personal security before officially hiring them. Because of the historical lack of statutory training requirements required in many states (Moore 1988), there remain openings for potential litigation. Indeed, an increase in negligent liability exposure has occurred in the forms of claims (Blackstone and Hakim 2010). Deficiencies in personnel hiring procedures only raise the chances of hiring a substandard

employee and increase risks of negligent hiring allegations (McCrie 2015). Courts do not take kindly to organizations' lack of accountability for not vetting their security applicants. There have been repeated rulings deeming that it is the responsibility of organizations to know whom they are hiring and if they are fit to carry out the proscribed duties for which they are responsible (Service 1988). Further, the employer is responsible for the acts committed by the employee under the legal doctrine "respondent superior" (Kaplan et al. 2012), which is a vicarious liability concept. Knowledge of the negligence or participation by the defendant is not even a necessary requirement to file a claim, illustrating the comprehensive dangers for employers. Through numerous rulings, the courts have outlined precisely how employers expose or raise risks of negligent hiring inside their organizations. Human resources personnel assigned the task of vetting personnel security should familiarize themselves with these delineated preventative measures. In basic terms, three requirements must exist to establish civil liability: (a) a legal duty by the plaintiff to protect the defendant, (b) a failure by the plaintiff to do so, and (c) damage or harm to the defendant as a result of that failure (McCrie 2015). Not conducting a thorough, competent background investigation that results in that subsequent harm certainly exposes companies to needless risk.

Conclusion

There exists the negative characterization that most private security professionals are uneducated and poorly paid (Kakalik and Wildhorn 1972). While this stereotype is not accurate, as most take their duties and responsibilities seriously (Lipman 1988), state regulation of private security is fragmented and loosely based (Bilek et al. 1981). There are precautions that organizations must take to protect themselves, which starts in the hiring process. The most critical influencer to creation of a competent and effective security culture is directly dependent on a belief of security importance by all parties involved (Connolly 2000). This point is especially true regarding organizations' employees and most importantly, its security employees. In the business realm, the importance of security is imperative to survival (Chia and Ruighaver 2002). When returns on investments result from smart security decision-making, that money can be used for other security and organizational projects (Vellani 2006).

Proper security staffing can be a time consuming, costly venture. There is likely aversion to these processes on the part of many organizational executives. Falling into that trap and taking the easy ways out may very well lead to more costs and wasted time later. A careful executive should realize that these vulnerabilities are not worth saving a few dollars at the inception. The hiring of top-quality professionals should be a top concern for stakeholders. Doing so will reflect well on the organization, reduce liability concerns, and increase cooperation and collaboration with local law enforcement. Failing to do so could result in detrimental effects for organization and their respective stakeholders.

Cross-References

- ▶ Corporate Security
- ▶ Personnel Security: Selection
- ▶ Security Management
- ▶ Security: Contract
- ▶ Security: Private
- ▶ Security: Proprietary

References

Adolf, D. (2011). Security studies and higher education. *Journal of Applied Security Research, 6*(1), 124–134.

Bayley, D., & Shearing, C. D. (2001). *The new structure of policing: Description, conceptualization and research agenda*. Washington, DC: National Institute of Justice.

Behar, R. (1992, March 9). Thugs in uniform. *Time, 139*(10).

Bilek, A. J., Klotter, J. C., & Federal, R. K. (1981). *Legal aspects of private security*. Cincinnati: Anderson.

Blackstone, E. A., & Hakim, S. (2010). Private policing: Experiences, evaluation, and future direction. In *Handbook on the economics of crime*. Northampton: Edward Edgar.

Brody, R. (2010). Beyond the basic background check: Hiring the "right" employees. *Management Research Review, 33*(3), 210–223.

Brown, T. S., Jones, J. W., Terris, W., & Steffy, B. D. (1987). The impact of pre-employment integrity testing on employee turnover and inventory shrinkage losses. *Journal of Business and Psychology, 2*(2), 136–149.
Bureau of Labor Statistics (BLS). (2010). *Security guards and gaming surveillance officers*. Retrieved from http://www.bls.gov
Bureau of Labor Statistics. (2018). *Occupational employment and wages, May 2018*. Retrieved from https://www.bls.gov/oes/current/oes339032.htm
Button, M., & George, B. (2005). Why some organisations prefer in-house to contract security staff. In M. Gill (Ed.), *Crime at work*. London: Palgrave Macmillan.
Center for Development of Security Excellence-Personnel Security. (2017). https://www.cdse.edu
Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). Understanding organizational security culture. *Proceedings of PACIS2002*. Japan, 158.
Cobbina, J. E., Nalla, M. K., & Bender, K. A. (2013). Security officers' attitudes towards training and their work environment. *Security Journal, 29*(3), 385.
Connolly, P. (2000). Security starts from within. *InfoWorld, 22*(28), 39–40.
Cunningham, W. C., & Strauchs, J. J. (1992). Security industry trends: 1993 and beyond. *Security Management, 36*(12), 27–30.
Fay, J. (2011). *Contemporary security management*. Burlington: Elsevier.
Gregory, P. (2015). *CISSP guide to security essentials*. Boston: Cenage.
Johnston, L., & Shearing, C. D. (2003). *Governing security: Explorations in policing and justice*. London: Routledge.
Kakalik, J. S., & Wildhorn, S. (1972). *The private police industry: Is nature and extent* (Vol. 2, p. 67). Santa Monica: The Rand Corporation.
Kaplan, J., Binder, G., & Weisberg, R. (2012). *Criminal law: Cases and materials* (7th ed.). New York: Wolters Kluwer Law & Business.
Lincke, S. (2015). Organizing personnel security. In *Security planning*. Cham: Springer.
Lipman, I. A. (1988). Personnel selection in the private security industry: More than just a resume. *American Academy of Political and Social Science, 498*(1), 83–90.
McAdams, A. C. (2004). Security and risk management: A fundamental business issue. *Information Management Journal, 38*(4), 36–44.
McCrie, R. (2015). *Security operations management*. Burlington: Butterworth-Heinemann.
Meadows, R. (1987). Negligence in the private guard industry. *Journal of Security Administration, 10*(2), 12–20.
Miles, D. (2012, June 21). Reforms improve DOD's security clearance process, official says. US Department of Defense. Retrieved from http://www.defense.gov
Mitrou, L., & Karyda, M. (2006). Employees' privacy vs. employers' security: Can they be balanced? *Telematics and Informatics, 23*(3), 164–178.
Moore, R. H., Jr. (1988). Civil liability for negligent and inadequate training: A private security problem. *Journal of Contemporary Criminal Justice, 4*(2), 106–118.
Nalla, M. K., & Crichlow, V. J. (2017). Have the standards for private security guards become more stringent in the post 9/11 era? An assessment of security guard regulations in the US from 1982 to 2010. *Security Journal, 30*(2), 523–537.
Nalla, M., & Hwang, E. (2006). Relations between police and private security officers in South Korea. *Policing, 29*(3), 482–497.
Nixon, R. (2016, May). Behind the backups at airport security. *New York Times*.
Ortmeier, P. J., & Johnson, B. R. (2017). *Introduction to security*. Pearson.
Papi, V. (1994). Hiring a security firm. *Journal of Property Management, 59*(2), 61–63.
Power, R., & Forte, D. (2006). Thwart the insider threat: A proactive approach to personnel security. *Computer Fraud & Security, 2006*(7), 10–15.
Rosenberg, J. (2007). Soft targets. *Journal of Property Management, 7*(4), 28–32.
Russell, D., & Arlow, P. (2015). *Industrial security: Managing security in the 21st century*. Hoboken: Wiley.
Sackett, P. R., & Harris, M. M. (1984). Honesty testing for personnel selection: A review and critique. *Personnel Psychology, 37*(2), 221–245.
Sennewald, C. A. (2011). *Effective security management* (5th ed.). Burlington: Butterworth-Heinemann.
Service, J. G. (1988, January). Negligent hiring: A liability trap. *Security Management*, p. 65.
Sissons, J. (2002). Advice for hiring security personnel. *Hotel & Motel Management, 217*(16), 72.
Stenning, P. C. (2000). Powers and accountability of private police. *European Journal on Criminal Policy and Research, 8*(3), 325–352.
UN News. (2011). https://news.un.org
Vellani, K. (2006). *Strategic security management*. Burlington: Elsevier.

Personnel Security: Recruitment

Maira Compagnone, Devon Hickman and Yalcin Acikgoz
Department of Psychology, Appalachian State University, Boone, NC, USA

Keywords
Recruitment · Hiring · Personnel security · Internal hires · Referrals · Intellectual property theft · Data security

Definition

Personnel security recruitment refers to activities that influence the number and types of applicants who apply for a security-related position, remain in the applicant pool, and accept an employment offer (Breaugh 2008).

Introduction

Traditionally, companies have relied on IT departments and firewalls to protect information, and employees have been viewed as the weakest link. Increasingly, however, companies are relying on employees to be the first line of defense, and thus human resources processes and policies are becoming imperative to protecting organizations from risks and violations of security. There are three major ways that employees can engage in security breaches in organizations. First, employees can be manipulated by outside influences such as hackers or phishing schemes. For example, in 2015, the US finance team at Ubiquiti made a multimillion dollar transfer for a senior executive, only to later find out that a criminal was posing as the executive (Sollars 2016). Second, employee negligence or error can lead to security breaches. In fact, 27% of all data breaches are caused by human error, versus 48% of breaches being caused by hackers or criminal insiders (IBM Security and Ponemon Institute 2018). Finally, the misuse of access to information, including theft, is another way employees can engage in security breaches.

Since it is frequently incumbents engaging in these violations, organizations can minimize the risk of such security violations by ensuring that individuals who are hired do not pose a security risk. While this is generally accomplished through utilizing appropriate screening methods during selection decisions, targeting individuals with the desired characteristics and treating them with consideration during the recruitment process can be an important first step. Accordingly, in this chapter, two methods of maximizing personnel security will be explored: (a) utilizing appropriate recruitment methods to target the desired candidates and (b) ensuring that applicants develop positive reactions to the organization.

Employee Recruitment

Employee recruitment refers to practices aimed at generating a qualified applicant pool, through strategic human resource planning (Mathis et al. 2017). In addition to attracting high-quality applicants who would likely perform well on the job, another organizational recruitment objective which specifically relates to personnel and people security involves attracting individuals who would not pose a threat to the organization's physical and intellectual assets. Depending on the type of position and/or organization, such as public or civil service, risks of violation may be deemed more or less severe and may necessitate greater consideration. Employee selection begins with the recruiting process. Accordingly, tailoring recruitment methods to attract applicants with the desired qualities, such as trustworthiness and reliability, may help organizations reach their security goals and thus have greater implications on the condition of the organization as a whole.

Goals of Employee Recruitment

Recruitment is the first essential element of talent acquisition. The overall objective of recruitment is to capture the attention of desired applicants and subsequently motivate these individuals to apply (Acikgoz 2019). Accordingly, the first step in the recruitment process is determining what the expected set of qualities are for an ideal applicant. This includes identifying the necessary knowledge, skills, abilities, and other characteristics, or KSAOs, by conducting a job analysis (Mathis et al. 2017). Employee trustworthiness and integrity are important aspects of applicant quality and job performance in any public or private organization, especially with regard to personnel security for companies with large intellectual repositories or physical assets. Organizations entrust their assets with the individuals they employ, and this requires a high level of trust between the individual and the

organization. In addition, organizations may wish to use the recruitment process to maximize applicant quality, diversity, job performance, job satisfaction, and employee retention while reducing the cost of hiring.

Once organizations have determined the key characteristics that are necessary for success on the job for vacant positions, the organization can gain a better picture of how to reach out to individuals with those attributes. In terms of ensuring personnel security, organizations can target individuals within certain characteristics who are likely to pose minimal risk. Strategic and targeted recruitment can aid in attracting individuals who can be entrusted with the physical and intellectual assets of an organization (Breaugh 2008). Various methods of recruitment, including internal job postings, employee referrals, and a focus on recruiter trustworthiness, are likely to be effective in accessing certain demographics, which will be explored in more depth in the next section.

Employee Recruitment Methods

According to Breaugh (2008), employee recruitment methods refer to any measures taken on behalf of an employer to provide potential applicants with an awareness of job openings. After determining recruitment objectives, recruiters can begin to design a strategy based on whom to recruit, where to recruit, what sources to use, and what message to communicate (Breaugh 2008). One distinction to be made in recruiting is between formal and informal methods, which are also referred to as direct and indirect methods. Formal methods are conventional routes taken by organizations to make professional contact with potential applicants, which include media advertisements, point of purchase methods, direct mail, employment agencies, college recruiters, computer databases, online job ads, and company websites. On the other hand, informal methods typically involve an applicant taking the initiative to contact an organization or a current member of the organization, organizations hiring from within by reaching out to their current or former employees, or a current employee referring a potential applicant for a job opening. Accordingly, informal methods include direct applications, employee referrals, and internal job postings.

A large body of research (Breaugh and Starke 2000; Castilla 2005; Zottoli and Wanous 2000) supports the advantages of informal methods, especially employee referrals and internal job postings. For example, employee-referred applicants are likely to have better job performance during the first 2 months of employment compared to those hired through formal methods. One reason for this phenomenon is that these employees have access to "difficult to obtain" information and face pressures from employees referring them to perform well (Castilla 2005). Internal hires can help to fill vacant positions in less time and thus with lower opportunity costs and financial costs than do external postings. Internal hires can also boost employee morale through the exemplification of workplace mobility. In addition, internal hires are more likely to be familiar with and aware of the corporate culture than external hires (Mathis et al. 2017). It is of little surprise that these methods lead to good post-hire outcomes, such as higher job performance and longer tenure than external hires (DeOrtentiis et al. 2018; Zottoli and Wanous 2000). The superiority stems from the fact that internal hires, especially employee referrals, are already vetted by the organization for competency and cultural fit before even entering the applicant pool, or in the case of hiring from within, the candidates are already well-known by the organization (Mathis et al. 2017).

In addition, internal promotion has been linked to higher levels of organizational commitment (Pinks 1992). Research (Dalal 2005; McClurg and Butler 2006) demonstrates a negative relationship between organizational commitment and counterproductive work behaviors. Counterproductive work behaviors are defined as intentional employee behaviors that are harmful to an organization's' interests and include areas of behavior such as theft and fraud (Dalal 2005). McClurg and Butler (2006) even proposed a conceptual model linking organizational commitment specifically to lowered instances of workplace theft. Accordingly, internal recruiting methods have

many positive outcomes for reducing security risks within an organization. Internal hires are indoctrinated to the organizational culture, and internal promotions increase organizational commitment. Internal hires generally have demonstrated performance capabilities and trustworthiness. Internal recruiting is thus an exceptional method for mitigating counterproductive or deviant work behaviors, such as theft, and reducing security risks within an organization.

Applicant Reactions

Applicant reactions refer to the attitudes, thoughts, or opinions formed by applicants regarding the organization during the recruitment and selection process (Ryan and Ployhart 2000). The reactions of the applicants can influence the decision to remain within the pool and potentially accept an offer (Turban and Cable 2003). Applicant reactions are influenced by personal characteristics, such as work experience, personality, and demographics but are also highly influenced by perceived procedure characteristics, job characteristics, and organizational context (Hausknecht et al. 2004). Organizations can foster positive reactions through recruitment procedures by considering the length and outcomes of the recruitment process and ensuring a fair treatment of the applicants during recruitment and selection. Positive reactions to the recruitment process (procedural justice perceptions) have a positive relationship with favorable organizational outcomes and organizational citizenship behaviors (Hausknecht et al. 2004). Organizational citizenship behaviors, or behaviors that an employee engages in that are unrewarded but nonetheless benefit an organization's performance, are negatively related to deviant work behaviors, such as theft or fraud (Dalal 2005). In addition, applicants with positive reactions to the recruitment process are less likely to leave the organization once hired. Garnering positive reactions from applicants will likely result in the retention of trustworthy and high-performance employees, in which the organization can invest time and money. Accordingly, by making sure that applicants have positive reactions during the recruitment and selection procedures, organizations can improve personnel security outcomes.

There are many ways organizations can improve applicant reactions during recruitment and selection. An applicant's perception of procedural characteristics influences overall judgments of fairness and general attitudes toward tests and selection. One facet of perceived procedural characteristics is job relatedness, which is composed of face validity and perceived predictive validity (Hausknecht et al. 2004). Face validity refers to the extent to which selection procedure content appears on the surface to be related to job content, whereas perceived predictive validity refers to the extent which selection procedure content seems to predict future job performance regardless of appearance. Face validity and perceived predictive validity are strong predictors of many applicant reactions, including procedural justice, referring to the fairness perceptions regarding the process through which selection decisions are made, and distributive justice, which refers to the perceived fairness of these decisions. These perceptions of justice have been found to predict several important outcomes, such as organizational attraction and intentions to litigate against an organization (Ababneh et al. 2014). In addition, applicants who hold positive perceptions about testing and selection in general are apt to view favorably those organizations using such tools.

Perceived procedural characteristics are positively related to applicants' perception of selection procedure fairness, which are related to overall attitudinal and behavioral outcomes (Hausknecht et al. 2004.) For example, research by Breaugh and Starke (2000) found that recruiters who appeared to be low on expertise and trustworthiness caused applicants to withdraw from the pool. In fact, it was found that individuals who viewed a recruiter as personable and trustworthy were more attracted to a position with the organization than those who perceived the recruiter to be low in those qualities (Chapman et al. 2005). If organizations are able to convey a culture of fairness and trustworthiness, applicants will be likely to reciprocate this virtue. In addition, researchers examining trustworthiness as a predictor of justice perceptions (Zapata et al. 2013) and on employee misconduct have found

that low perceptions of justice are a leading indicator of workplace theft (Jex and Britt 2008). This correlation may occur because employees frustrated with organizational procedures attempt to take control the situation by engaging in deviant behaviors.

Measuring Effectiveness

Metrics of recruitment effectiveness can be divided into two domains – the objectives that are fulfilled either pre- or post-hire. Pre-hire measures include the number of applicants, quality of applicants, and the reactions generated. Some post-hire measures are cost and time to fill positions, first-year hire retention rates, job performance, and diversity impact. Evaluation results should demonstrate the value of the recruitment methods used in regard to attainment of organizational goals and should be used to further improve the recruitment process within the organization by increasing cost/time efficiency. Organizations with high risk of data violations or personnel security risks may also evaluate their recruitment efforts in terms of organizational outcomes that pertain to the mitigation of those risks. For example, organizations can examine whether employees coming from a specific recruitment source tend to be more or less likely to engage in security violations and compare results across various methods. Metrics on recruitment methods can be used in comparison to various organizational outcomes to rate the effectiveness of specific methods and increase the likelihood of attracting talent that meets organizational goals.

Conclusion

Recruitment is the first step in acquiring quality employees and ensuring the prosperity of an organization. A wide variety of methods are available, making it important that an employer identifies the value and desired outcomes of filling any vacancy before deciding how to implement the process. Some positions are of higher importance than others, which often equates to a need to have strict safety requirements. However, personnel security violations exist as a potential risk for many position levels in a corporate environment. Though there is no way to completely eradicate personnel security risks, taking applicant reliability into consideration during the recruitment process can significantly reduce the likelihood of violations.

Cross-References

- ▶ Interviewing Adults: Communication at the Front Line
- ▶ Personnel Security: Hiring
- ▶ Personnel Security: Retention
- ▶ Personnel Security: Selection

References

Ababneh, K. I., Hackett, R. D., & Schat, A. H. (2014). The role of attributions and fairness in understanding job applicant reactions to selection procedures and decisions. *Journal of Business and Psychology, 29*(1), 111–129. https://doi.org/10.1007/s10869-013-9304-y.

Acikgoz, Y. (2019). Employee recruitment and job search: Towards a multi-level integration. *Human Resource Management Review, 29*(1), 1–13. https://doi.org/10.1016/j.hrmr.2018.02.009.

Breaugh, J. A. (2008). Employee recruitment: Current knowledge and important areas for future research. *Human Resource Management Review, 18*(3), 103–118. https://doi.org/10.1016/j.hrmr.2008.07.003.

Breaugh, J. A., & Starke, M. (2000). Research on employee recruitment: So many studies, so many remaining questions. *Journal of Management, 26*(3), 405–434. https://doi.org/10.1177/014920630002600303.

Castilla, E. J. (2005). Social networks and employee performance in a call center. *American Journal of Sociology, 110*(5), 1243–1283.

Chapman, D. S., Uggerslev, K. L., Carroll, S. A., Piasentin, K. A., & Jones, D. A. (2005). Applicant attraction to organizations and job choice: a meta-analytic review of the correlates of recruiting outcomes. *Journal of Applied Psychology, 90*(5), 928.

Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology, 90*(6), 1241–1255. https://doi.org/10.1037/0021-9010.90.6.1241.

DeOrtentiis, P. S., Van Iddekinge, C. H., Ployhart, R. E., & Heetderks, T. D. (2018). Build or buy? The individual and unit-level performance of internally versus

externally selected managers over time. *Journal of Applied Psychology, 103*(8), 916–928. https://doi.org/10.1037/apl0000312.
Hausknecht, J. P., Day, D. V., & Thomas, S. C. (2004). Applicant reactions to selection procedures: An updated model and meta-analysis. *Personnel Psychology, 57*(3), 639–683. https://doi.org/10.1111/j.1744-6570.2004.00003.x.
Jex, S. M., & Britt, T. W. (2008). *Organizational psychology a scientist-practitioner approach* (2nd ed.). Hoboken: Wiley.
Mathis, R., Jackson, J., Valentine, S., & Meglich, P. (2017). *Human resource management*. Boston: Cengage Learning.
McClurg, L. A., & Butler, D. S. (2006). Workplace theft: A proposed model and research agenda. *Southern Business Review, 31*(2), 25–34.
Pinks, G. J. (1992). Facilitating organizational commitment through human resource practices. In *Personnel management* (pp. 1–24). Kingston: Hewson & White Printing Ltd.
Ponemon Institute. (2018). Ponemon institute – The 2018 cost of a data breach study by the Ponemon institute. IBM security services. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&
Ryan, A., & Ployhart, R. E. (2000). Applicants' perceptions of selection procedures and decisions: A critical review and agenda for the future. *Journal of Management, 26*(3), 565–606. https://doi.org/10.1016/s0149-2063(00)00041-6.
Sollars, M. (2016). Risk-based security: Staff can play the defining role in securing assets. *Network Security, 2016*(9), 9–12. https://doi.org/10.1016/S1353-4858(16)30087-3.
Turban, D. B., & Cable, D. M. (2003). Firm reputation and applicant pool characteristics. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 24*(6), 733–751. https://doi.org/10.1002/job.215.
Zapata, C. P., Olsen, J. E., & Martins, L. L. (2013). Social exchange from the supervisor's perspective: Employee trustworthiness as a predictor of interpersonal and informational justice. *Organizational Behavior and Human Decision Processes, 121*(1), 1–12. https://doi.org/10.1016/j.obhdp.2012.11.001.
Zottoli, M. A., & Wanous, J. P. (2000). Recruitment source research: Current status and future directions. *Human Resource Management Review, 10*(4), 353–382. https://doi.org/10.1016/S1053-4822(00)00032-2.

Further Reading

Acikgozy, Y. & Bergman, S. M. (2016). Social media and employee recruitment: Chasing the run away bandwagon. In R. N. Landers, G. B. Schmidt, R. N. Landers, G. B. Schmidt (Eds.), Social media in employee selection and recruitment: Theory, practice, and current challenges, Springer International Publishing, Cham, Switzerland (2016), pp. 175–195
Gully, S. M., Phillips, J. M., Castellano, W.G., Han, K. & Kim, A. (2013). A mediated moderation model of recruiting socially and environmentally responsible job applicants. *Personnel Psychology, 66*(4), 935–973, https://doi.org/10.1111/peps.12033
Phillips, J. M., & Gully, S. M. (2015). Multilevel and strategic recruiting: Where have we been, where can we go from here? *Journal of Management, 41*(5), 1416–1445, https://doi.org/10.1177/0149206315582248

Personnel Security: Retention

M. M. Laske, Maira Compagnone and Yalcin Acikgoz
Department of Psychology, Appalachian State University, Boone, NC, USA

Keywords
Retention · Personnel security · Turnover · Job satisfaction · Talent management

Definition

Personnel security	Policies and procedures aimed at mitigating the risk of employees exploiting their access to an organization's resources for purposes outside of their employment purview
People security	Relates to the organizational environment and security culture
Retention	"Actions to keep employees motivated and focused so they elect to remain employed and fully productive for the benefit of the organization" (SHRM 2019)
Attrition	"The overall reduction in the workforce, including vacancies that go unfilled and jobs that are eliminated" (Sonsino 2017)

Commitment	"The sense of dedication that employees feel toward the companies and organizations they work for" (Kivak 2019)
Organizational citizenship behavior	"Individual behavior that is discretionary, not directly or explicitly recognized by the formal reward system, and that in the aggregate promotes the effective functioning of the organization" (Organ 1988, p. 4)
Counterproductive work behavior	"Behavior that explicitly runs counter to the goals of the organization" (Jex and Britt 2008, p. 168)
Job satisfaction	"The extent to which people like (satisfaction) or dislike (dissatisfaction) their jobs" (Spector 1997, p. 2)

Introduction

Retaining employees and reducing employee turnover is of importance for the promotion of personnel security. In 2018, there were 40.1 million separations in which employees voluntarily initiated the change, while there were 21.9 million layoffs or discharges for the same time span (U.S. Bureau of Labor Statistics [BLS] 2019b, March). These data indicate that employees are leaving positions at a greater rate than they are being laid off or discharged. It should also be noted that the job opportunities have been increasing since July of 2009 and reached a peak of 7.3 million openings in December of 2018 (BLS 2019a, February). This could indicate that organizations not only have to be concerned about turnover costs, which are estimated at $567 billion annually (Working Institute 2018), but also about retaining high-quality personnel.

In addition to the financial burden of losing qualified employees as a result of voluntary turnover, retention is also important because with every replacement comes a new employee who is not yet as well-known and trusted as the employee who is replaced. This may bring some personnel security threats, which may include such actions as theft, workplace sabotage, and misuse of company resources, which can be quite costly. In fact, 6% of employees reported knowledge of fraudulent, illegal, or unethical activities in 2017, an increase from 1% in 2010 (Work Institute 2018). These data indicate a growing concern regarding personnel security among organizations. Although these reports do not specify the number of these occurrences, data are available on the costs of such misuses of company resources. For example, the average total cost of a data breach in the United States is estimated to be close to $8 million, while the average cost of a single lost/stolen record is $233 for the United States (Ponemon Institute 2018). Because of these substantial costs, reducing employee turnover and increasing retention of loyal and highly competent employees are of importance. Strategies to promote retention and therefore reduce potential issues of personnel security include increasing organizational commitment, focusing on talent management, and increasing job satisfaction. These areas of focus can help organizations retain top, trusted talent and thus reduce security concerns related to personnel.

Turnover

An important distinction in terms of employee retention can be made between optimal and dysfunctional turnover. Not all turnover is created equal, as there are times when it may make financial sense to have someone leave an organization. Optimal turnover occurs when poor performing or untrustworthy employees voluntarily leave an organization, whereas dysfunctional turnover refers to high performing employees, the talent that organizations want to keep, leaving an organization. Dysfunctional turnover is the type of turnover that needs to be addressed through the development of retention strategies. These employees may react to financial incentives, but often the decision to leave a company is made because of other concerns, such as the

organizational culture, opportunities for promotion and development, supervisors, location, or even familial concerns. Organizations can minimize the impact of some of these extraneous variables by focusing on effective talent management strategies and tactics to increase job satisfaction. These strategies will increase organizational commitment, loyalty, and thus retention within the organization.

Antecedents of Retention

Organizations, through the attention they provide their employees with, can develop emotional bonds between the organization and the employee, known as social bonds (McClurg and Butler 2006). These affective components, or feelings of attachment to an organization, are part of organizational commitment (Mathieu and Zajac 1990). Organizational commitment was shown to be negatively related with intentions to search for other employment opportunities and intentions to leave an organization (Mathieu and Zajac 1990), especially when employees have high perceptions of employability (Acikgoz et al. 2016). In addition, research consistently shows that employees with more ties to an organization, whether those ties are demonstrated through (a) their tenure, (b) their lack of turnover intention, or (c) their organizational commitment, are less likely to steal (McClurg and Butler 2006). Work engagement, or employee engagement, takes organizational commitment a step further, and states that as a result of the emotional bond with the organization, employees are more likely to engage in acts that further the organizational goals, through vigor, dedication, and absorption (Schaufeli et al. 2002). Work engagement is related to a number of beneficial organizational outcomes, including improved job performance, increased effort, innovation, and higher numbers of organizational citizenship behaviors (Pandita and Ray 2018).

Three top drivers of work engagement include (a) the opportunity to use skill sets, (b) alignment between employee and employer values, and (c) the belief that the employee's efforts will make a difference in the organization (Johnson and Pike 2018). These drivers can be greatly impacted by two important antecedents of work engagement: effective talent management strategies and job satisfaction.

Talent Management

Talent management is a very broad term that covers many general human resource duties that are mainly concerned with attracting and keeping top talent within an organization, which includes methods that increase employee engagement. One of the most impactful ways that organizations can retain top talent and combat dysfunctional turnover is through workforce development. In fact, the Work Institute's 2018 Retention Report found that the top reason employees left their jobs was related to a lack of development opportunities (21%), along with work-life balance concerns (13%), and manager behavior (11%). Thus, a focus on career planning, development, and training can significantly reduce employees' desire to turn to another company for those opportunities. Successful employee development programs should include a diverse mix of some of the following strategies: coaching, mentoring, individual development plans, talent assessments, "stretch" assignments, job enrichment, job shadowing, job rotation, and succession planning. These strategies allow employees to explore different roles within the organization, test out new ideas, and develop skills that will allow for positive career growth. Some organizations are under the mistaken impression that developing employees will lead to attrition, as employees receive skills that are highly transferable in the external labor market. However, research has shown that skill utilization obtained from development opportunities leads to a decrease in employee turnover intentions (Nelissen et al. 2017). This is a considerable finding as employee intentions to quit are strong predictors of actual turnover (Griffeth et al. 2000). Organizations can also increase the retention of top performers by matching skill set improvements with an increase in compensation, commensurate to the

employee's external value in the relevant labor market (Anis et al. 2011). By focusing on developing top talent and increasing employee engagement, organizations can reduce turnover and retain employees who are proven performers with organizational loyalty, which in turn means retaining the employees who are known and trusted. These employees will be less of a risk for potential concerns surrounding personnel security.

Job Satisfaction

Job satisfaction is defined as "the extent to which people like (satisfaction) or dislike (dissatisfaction) their jobs" (Spector 1997, p. 2). It may seem like common sense to insinuate that a happy worker is a good worker, but the relationship between job satisfaction and superior workplace outcomes is more complicated. More than the reduction to "happy," or "satisfied," job satisfaction is comprised of affective, cognitive, and behavioral components (Judge et al. 2001). Affective satisfaction represents the employee's feelings toward their work and their employer, while cognitive satisfaction is represented by the employee's beliefs about their job and employer (such as believing that a job is boring or stimulating). Affective and cognitive evaluations about the quality of work are often dependent on one another. The belief that a job is too menial or repetitive, for example, may lead an employee to have a negative affect or disposition toward the work. Behavioral tendencies, represented within the behavioral component of satisfaction, such as regular attendance to work or high job performance, may reveal job satisfaction in a different way. The interaction of these three components is often why the cliché statement "a happy worker is a hard worker" is so often espoused. Employees who have positive beliefs about their employer and their job will generally have more positive affect toward their job, which will lead to better citizenship behaviors within the workplace.

Due to the high financial costs of turnover and potential of misuses of company information upon termination, it is important to increase employee job satisfaction, as it is related with lower instances of turnover (Carsten and Spector 1987; Valentine et al. 2011). Employees high in job satisfaction are also more likely to engage in the culture-building behaviors that will promote the values and culture that an organization wishes to foster. Dalal (2005) found that job satisfaction was related to lower instances of counterproductive work behaviors. These findings support the idea that higher job satisfaction will lead to organizational commitment and lower rates of turnover.

A number of organizational initiatives can increase job satisfaction among employees. Specifically, job satisfaction is influenced by (a) perceptions of fairness in terms of organizational procedures, (b) levels of respect and trust between employees and senior management, (c) pay commensurate with skills and abilities, (d) the opportunity to demonstrate skills and abilities, and (e) job security (SHRM 2019). The next section covers examples of strategies of talent management and employee engagement to improve retention.

Examples of Strategies

Employee perceptions of the decision-making process within an organization can be directly linked to the levels of trust and respect an employee may have with both their supervisors and organization representatives. Perceptions of fairness can be improved with fair compensation for work but can also be increased through open communication channels between worker and management, recognition of good work, and opportunities to develop and grow within an organization, which can convey job security to an employee. Distributive justice, or perceptions about the fairness of organizational decisions, as well as procedural justice, which is the perception of fairness of the process through which organizations make decisions, can reduce counterproductive work behaviors. In a study by Spector (1997), it was found that deviant behaviors such as theft can arise from feelings of frustration within an organization, in reaction to low

perceptions of fairness or representation in the decision-making processes. In addition, it has previously been found that inadequate communication resulted in increased rates of theft and greater amounts of turnover (Greenberg 1990; Ralph and Holmvall 2016). These findings suggest that increasing employee job satisfaction is a crucial step in personnel security for improving retention rates of employees and reducing counterproductive work behaviors detrimental to the organization.

Improving the relationship between employees and supervisors and thus increasing leadership effectiveness is another strategy to improve job satisfaction and, therefore, reduce turnover. Specifically, behaviors such as monitoring employees and providing consequences, providing opportunities to discuss evaluations, giving personalized feedback, giving positive comments about work, and helping employees with goal setting are examples of actions that leaders can engage in to improve job satisfaction of employees (Komaki 1998; Komaki and Minnich 2016). Komaki and Minnich (2016) found that such behaviors led to an increase in job satisfaction, which resulted in improved organization climate and an increase in intentions to stay with the organization.

As previously mentioned, skill utilization has a negative relationship with turnover intentions (Nelissen et al. 2017). An additional benefit of skill utilization is that it is highly correlated with job satisfaction (Humphrys and O'Brien 1986; Tian et al. 2018). Therefore, focusing on developing employees and providing them opportunities to utilize their skills will lead to greater rates of job satisfaction and retention within an organization. Monitoring and developing skills of employees also provides opportunities for managers to provide contingent consequences that have been found to improve employee satisfaction (Komaki 1998; Komaki and Minnich 2016).

An additional strategy to improve employee retention is to measure employee job satisfaction and organizational commitment continually. An annual survey on either of these facets may not be frequent enough and allows employee information regarding satisfaction and organizational commitment to go unaccounted for if they leave the organization (Lee et al. 2018). While it is possible that an organization can develop its own measures of job satisfaction and organizational commitment, measures are also available in both the academic literature (e.g., Minnesota Satisfaction Questionnaire, Weiss et al. 1967; Organizational Commitment Scale, Meyer et al. 1993) and from companies specialized in developing these assessments. Monitoring changes in employee commitment and satisfaction more consistently and continually will allow for quicker identification of turnover intentions in an organization. Being able to adapt swiftly to data collected from organizational commitment and job satisfaction measures will allow for better management of retention in an organization.

Conclusion

Retaining employees in positions that are at higher risks in terms of personnel security is crucial for success of an organization. Improving engagement in the workforce through talent management and increasing job satisfaction are two areas to focus on to improve retention. As the number of job opportunities available and employee turnover increases, strategies to improve employee satisfaction become even more critical. Improving (a) perceptions of fairness, (b) employee supervisor relationships, (c) employee development and skill utilization, and (d) frequently monitoring organizational commitment and employee satisfaction are all strategies organizations should use to improve retention of their employees.

Cross-References

- ▶ Personnel Security: Recruitment
- ▶ Personnel Security: Selection

References

Acikgoz, Y., Sumer, H. C., & Sumer, N. (2016). Do employees leave just because they can? Examining the perceived employability–turnover intentions

relationship. *Journal of Psychology: Interdisciplinary and Applied, 150*(5), 666–683. https://doi.org/10.1080/00223980.2016.1160023.

Anis, A., Nasir, A., & Safwan, N. (2011). Employee retention relationship to training and development: A compensation perspective. *African Journal of Business Management, 5*(7), 2679–2685. https://doi.org/10.5897/AJBM10.1036.

Carsten, J. M., & Spector, P. E. (1987). Unemployment, job satisfaction, and employee turnover: A meta-analytic test of the Muchinsky model. *Journal of Applied Psychology, 72*(3), 374–381. https://doi.org/10.1037/0021-9010.72.3.374.

Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology, 90*(6), 1241–1255. https://doi.org/10.1037/0021-9010.90.6.1241.

Greenberg, J. (1990). Employee theft as a response to underemployment inequity: The hidden costs of pay cuts. *Journal of Applied Psychology, 75*(5), 561–568. https://doi.org/10.1037/0021-9010.75.5.561.

Griffeth, R. W., Hom, P. W., & Gaertner, S. (2000). A meta-analysis of antecedents and correlates of employee turnover: Update, moderator tests, and research implications for the next millennium. *Journal of Management, 26*(3), 463–488. https://doi.org/10.1177/014920630002600305.

Humphrys, P., & O'Brien, G. E. (1986). The relationship between skill utilization, professional orientation and job satisfaction for pharmacists. *Journal of Occupational Psychology, 59*(4), 315–326. https://doi.org/10.1111/j.2044-8325.1986.tb00232.x.

Jex, S. M., & Britt, T. W. (2008). *Organizational psychology: A scientist-practitioner approach* (2nd ed.). Hoboken: Wiley.

Johnson, S., & Pike, B. (2018). The state of engagement in public accounting firms and why it matters. *CPA Journal, 88*(12), 64–66.

Judge, T. A., Thoresen, C. J., Bono, J. E., & Patton, G. K. (2001). The job satisfaction-job performance relationship: A qualitative and quantitative review. *Psychological Bulletin, 127*(3), 376–407. https://doi.org/10.1037//0033-2909.I27.3.376.

Kivak, R. (2019). Organizational commitment. In *Salem Press encyclopedia*. Retrieved from http://search.ebscohost.com.proxy006.nclive.org/login.aspx?direct=true&db=ers&AN=121772893&site=eds-live&scope=site

Komaki, J. L. (1998). *Leadership from an operant perspective*. London: Routledge.

Komaki, J. L., & Minnich, M. L. R. (2016). A behavioral approach to organizational change: Reinforcing those responsible for facilitating the climate and hence promoting diversity. *Journal of Organizational Behavior Management, 36*(2–3), 154–184. https://doi.org/10.1080/01608061.2016.1200514.

Lee, T. W., Hom, P., Eberly, M., & Li, J. J. (2018). Managing employee retention and turnover with 21st century ideas. *Organizational Dynamics, 47*(2), 88–98. https://doi.org/10.1016/j.orgdyn.2017.08.004.

Mathieu, J. E., & Zajac, D. M. (1990). A review and meta-analysis of the antecedents, correlates, and consequences of organizational commitment. *Psychological Bulletin, 108*(2), 171–194. https://doi.org/10.1037/0033-2909.108.2.171.

McClurg, L. A., & Butler, D. S. (2006). Workplace theft: A proposed model and research agenda. *Southern Business Review, 31*(2), 25–34.

Meyer, J. P., Allen, N. J., & Smith, C. A. (1993). Commitment to organizations and occupations: Extension and test of a three-component conceptualization. *Journal of Applied Psychology, 78*(4), 538–551. https://doi.org/10.1037/0021-9010.78.4.538.

Nelissen, J., Forrier, A., & Verbruggen, M. (2017). Employee development and voluntary turnover: Testing the employability paradox. *Human Resource Management Journal, 27*(1), 152–168. https://doi.org/10.1111/1748-8583.12136.

Organ, D. W. (1988). *Organizational citizenship behavior: The good soldier syndrome*. Lexington: Lexington Books.

Pandita, D., & Ray, S. (2018). Talent management and employee engagement – A meta-analysis of their impact on talent retention. *Industrial and Commercial Training, 50*(4), 185–199. https://doi.org/10.1108/ICT-09-2017-0073.

Ponemon Institute. (2018, July). *2018 Cost of a data breach study: Global overview. IBM Security Services*. Traverse City. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

Ralph, C. D. S., & Holmvall, C. M. (2016). Examining the relationship between the justice facets and turnover intent: The mediating roles of overall justice and psychological strain. *Military Psychology, 28*(4), 251–270. https://doi.org/10.1037/mil0000104.

Schaufeli, W. B., Salanova, M., Gonzalez-Roma, V., & Bakker, A. B. (2002). The measurement of engagement and burnout: A two sample confirmatory factor analytic approach. *Journal of Happiness Studies, 3*, 71–92.

Society for Human Resource Management. (2019). *Managing for employee retention*. Society for Human Resource Management. Retrieved from https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/managingforemployeeretention.aspx

Sonsino, D. (2017). *Viewpoint: Does attrition still matter?* Society for Human Resource Management. Retrieved from https://www.shrm.org/hr-today/news/hr-magazine/1017/pages/does-attrition-still-matter.aspx

Spector, P. E. (1997). *Job satisfaction: Application, assessment, causes, and consequences*. Thousand Oaks: Sage. https://doi.org/10.4135/9781452231549.

Tian, A. W., Wang, Y., & Chia, T. (2018). Put my skills to use? Understanding the joint effect of job security and skill utilization on job satisfaction between skilled migrants and Australian born workers in Australia. *Social Indicators Research, 139*(1), 259–275. https://doi.org/10.1007/s11205-016-1404-4.

U.S. Bureau of Labor Statistics. (2019a, February 12). *Job openings and labor turnover – December 2018 – USDL-*

19-0240. Retrieved from U.S. Bureau of Labor Statistics https://www.bls.gov/news.release/pdf/jolts.pdf

U.S. Bureau of Labor Statistics. (2019b, March 15). *Job openings and labor turnover – January 2019 – USDL-19-0404*. Retrieved from U.S. Bureau of Labor Statistics https://www.bls.gov/news.release/pdf/jolts.pdf

Valentine, S., Godkin, L., Fleischman, G. M., & Kidwell, R. (2011). Corporate ethical values, group creativity, job satisfaction and turnover intention: The impact of work context on work response. *Journal of Business Ethics, 98*(3), 353–372. https://doi.org/10.1007/s10551-010-0554-6.

Weiss, D. J., Dawis, R. V., & England, G. W. (1967). *Manual for the Minnesota Satisfaction Questionnaire*. Minneapolis: University of Minnesota.

Work Institute. (2018). *2018 Retention report truth & trends in turnover*. Franklin. Retrieved from https://cdn2.hubspot.net/hubfs/478187/2018%20Retention%20Report/Work%20Institute%202018%20Retention%20Report%20043018%20-%20Final.pdf?__hssc=163589856.2.1544530382638&__hstc=163589856.e72e42ce0b71f3ce20acc3965c52e917.154453038263 7.1544530382637.1544530382637.1&__hsfp=16946

Further Reading

Meyer, J. P., & Allen, N. J. (1997). *Commitment in the workplace: Theory, research, and application*. Thousand Oaks: Sage.

Spector, P. E. (1997). *Job satisfaction: Application, assessment, causes, and consequences*. Thousand Oaks: Sage. https://doi.org/10.4135/9781452231549.

Personnel Security: Selection

Haiden Weaver and Yalcin Acikgoz
Department of Psychology, Appalachian State University, Boone, NC, USA

Keywords

Selection · Hiring · Validity · Reliability · Background check

Definition

Personnel security selection refers to the methodical process of determining which security position candidates to hire.

Introduction

Personnel selection has, over time, transitioned from an intuitive process based on gut feelings and unsound logic into an empirical process. This process utilizes scientific methods and modern techniques to ensure that an organization makes an objective best fit decision when deciding to hire a new employee or promote from within. Overall, there are three major categories of selection tests that can be performed to evaluate a candidate: classical methods, job analysis-based tests, and security tests. Using these methods, candidates are assessed, and their scores are compared. Depending on the needs of the organization, a selection method is then utilized to determine which candidates are the best fit for the position and organization (Spector 2012).

In addition to poor job performance, consequences of making a bad hiring decision could be hiring an employee who will exhibit counterproductive behaviors such as theft, sabotage, sharing intellectual property without authorization, or even violence, all of which represent a huge cost and liability to the organization (van Zyl and de Bruin 2018). Counterproductive work behaviors refer to volitional acts by employees that potentially violate the legitimate interests of, or do harm to, any organization or its stakeholders (Marcus et al. 2016). However, these risks can be mitigated by having a proper selection battery that includes security tests. The degree to which security tests are utilized in such a battery and the importance placed on them depends on the job offered and organizational requirements. For example, when hiring for a critical position such as a job with access to high-level information, security tests may be given a higher weight.

Additionally, in order to help promote organizational security, the security supervisor of the organization should have an active role during the selection process. The security supervisor may have different titles depending on the type and size of the organization, but they are the individuals responsible for creating and/or implementing security standards and procedures as well as identifying, investigating, and resolving any breaches in security. In addition, security

managers are generally in a position to monitor other employees and customers to ensure safety and security of the organization. Accordingly, it is important to involve the security supervisor throughout the process so that they can better contextualize selection battery responses to identify candidates who may potentially pose a threat to the organization (National Center for O∗NET Development 2018). Regardless of what type of selection test is used, it is important that it is reliable and valid in predicting desired outcomes such as high levels of job performance or a low risk for the organization. A test or method is considered reliable if it produces accurate, reproducible, and consistent results. Similarly, a test or method has validity if it assesses the dimension it is supposed to measure and therefore predicts outcomes that it is expected to predict (Spector 2012).

Types of Selection Tests

When choosing which selection tests to utilize, there are several factors to consider. First, a decision must be made regarding which tests are the most relevant to the position based on the position's regular activities, tools and equipment used, and other job specifications (Doverspike and Arthur 2012). This information should be derived from the position's job analysis. If no analysis exists for the position, one should be performed before selecting a candidate to fill that position (Spector 2012). Since job analysis involves obtaining information about a job from subject matter experts, which may include employees or supervisors working in a job, it is important that the security manager is involved in analyses of security-related jobs. Next, the selection tests to be used in hiring must be determined such that each selection test should measure one or more competencies necessary for that position. Below, each of the three broad categories of selection tests – classical methods, job-specific tests, and security tests – are discussed in more detail.

Classical Methods

Examples of classical selection testing methods include the interview, resume or application review, and reference evaluations. Each of these methods were developed as part of the original intuitive process that used to dominate personnel selection. However, these methods have since evolved into empirical tools that are scientifically developed and used by organizations to make more efficient selection decisions. Part of the reason these methods have remained popular is that they continue to most effectively measure person-organization fit, that is, the degree of compatibility between an individual and the values and culture of the organization (Kristof 1996; US Office of Personnel Management 2019b). Due to these methods being best suited to measure person-organization fit, they are commonly used in the hiring of new employees. However, classical methods still exhibit a useful level of validity in determining person-job fit, which refers to the degree of compatibility between an individual and the tasks and responsibilities she or he must be able to perform as part of the job (Kristof-Brown and Guay 2011). This most commonly takes the form of a structured interview being used to evaluate candidates for a promotion or job change within an organization they are already members of. Interviews can also be used by the security manager as a way to assess a candidate in the hiring process. In this instance, the security supervisor will be able to physically observe the candidate as they provide responses. This provides the security supervisor, through interpreting tone, language, and body language of the candidate, a better sense of it if the candidate may be lying or committing impression management (Sebanz and Shiffrar 2009).

Classical methods, especially the structured interview, demonstrate high reliability and validity for determining if a candidate has the characteristics and values desired by the organization. However, it is important to note that each structured interview will have its own associated validity and reliability based on the questions asked and the scoring system used. Structured interviews ideally must have the following characteristics: (1) the test must include the same set of questions asked to each candidate, (2) the questions must be relevant to the requirements of the job and the values of the organization, (3) the

questions must not involve information protected under the US Equal Employment Opportunity Commission, and (4) answers to each question must be evaluated objectively based on a predetermined system. In addition to higher validity, classical methods are also associated with lower evaluation costs. Cost per candidate refers to the monetary value associated with developing or buying, administering, and scoring a selection test to a group of candidates over the number of expected candidates. The structured interview requires the most intensive development of the classical methods and still presents a relatively small overhead cost. Other classical methods such as the resume or reference review cost little to no overhead. The only remaining cost associated with classical methods is the value of the time used by an employee to conduct the interview or review and analyze the results of the interview, resume/application, and references. The combined aspects of higher effectiveness, determined as a result of a test's validity and reliability, with a low cost per applicant are what make these classical methods still so appealing to organizations (US Office of Personnel Management 2019).

Job Specific

Job-specific tests are the most varied type of personnel selection tests because they are entirely dependent on the job being performed. Examples of job-specific tests are cognitive ability tests, physical ability tests, or work sample tests. It is important to ensure that the person hired is actually capable of performing the job they were hired to do. These types of selection tests are used to measure the capabilities that are found to be needed in a job through a job analysis. These methods were created over time as a result of the development of the scientific nature of human resources management and industrial and organizational psychology. Hence, the purpose of job-specific tests is to scientifically measure person-job fit in terms of whether a candidate possesses the knowledge, skills, abilities, or other characteristics (KSAOs) required for a job. Accordingly, these tests tend to demonstrate high validity for determining if a candidate will perform a specific job well. Other benefits of job-specific tests are that they are the least susceptible to impression management and fake responses, they can be used to provide developmental feedback, and they also provide applicants with a realistic preview of the job (Thornton and Kedharnath 2013). Despite all these benefits, some job-specific tests such as cognitive ability tests can create moderate to high levels of adverse impact, which refers to the problem of producing different results for candidates who are members of a minority group compared to members of a majority group (Oostrom and De Soete 2016).

Job-specific selection tests can be critical in hiring of security personnel. Security personnel are typically hired for either physical security positions such as security guards or for digital security jobs such as an information technology and data security analyst. Though both roles are security oriented, they have different responsibilities and require different knowledge, skills, and abilities. Perhaps more so than most jobs in an organization, it is crucial that security personnel are able to perform their job duties with a high degree of proficiency (National Center for O∗NET Development 2019a, b). Accordingly, it is important that appropriate job-specific selection tests are utilized when hiring personnel for security-related positions.

Security

Security tests comprise the third major category of selection tests and are valuable not just for mitigating potential security risks but also as a valid predictor of the overall job performance. Examples of security tests are integrity tests and background checks. These types of selection tests may provide the most utility in preventing the organization from hiring a high-risk employee, such as one who might steal, sabotage, or become violent. However, other types of selection tests can be adapted to be used as a security test as well, such as an integrity test taking the form of a structured interview.

Integrity tests have good validity in predicting job performance and are consequently one of the most commonly used security tests (Sydell (n.d.)). These are typically applied in a paper-pencil format and include questions assessing attitudes

toward counterproductive behaviors. Low scores on an integrity test are associated with counterproductive behaviors in the organization such as theft, sabotage, disciplinary problems, absenteeism, and even violence. Integrity tests have low levels adverse impact and can be effectively paired with a test that has a higher adverse impact such as the cognitive ability test in order to reduce the overall group differences in a selection battery (Ones et al. 2012; US Office of Personnel Management 2019). Additionally, integrity tests are cost-effective and easy to administer. However, when applied in a written form, integrity tests are susceptible to candidates giving false answers to make themselves appear more favorably, also known as impression management. Even though polygraph machines can also be utilized to assess integrity, they are not allowed to be utilized as a method of employee selection for most private organizations under the Employee Polygraph Protection Act or 1988. Although exceptions exist under this law, these exceptions only cover jobs with government entities, security firms, or pharmaceutical manufacturers, distributors, and dispensers.

Background checks, the most common type of security tests, are implemented by 86% of organizations to find out if candidates have previously engaged in counterproductive behaviors (Aamodt 2015). There are two major types of background checks: criminal history checks and credit history checks. However, the pervasiveness of the Internet is leading some organizations to now use social media as a form of background screening. In addition to these methods, background checks can be so expansive as to include driving records, work history, military service, and education records (Aamodt 2015). This section will focus on the two primary types of background checks as well as the emerging prevalence of using social media as a background screening tool.

Credit history checks are the less prominent of the two major types and tend to include previous addresses, court-ordered judgments, list of revolving accounts with payment history and current balances, and installment accounts with payment history and current balances. This information is always obtained from the same three major credit reporting agencies in the United States. These checks are entirely financially oriented and are typically only administered when the position requires handling large amounts of money or other financial information such as budgeting. Credit checks have high face validity, the degree to which they appear to be effective, for financial positions and serve as a predictor of conscientiousness, responsibility, and some counterproductive behaviors such as absenteeism and theft. However, they have little-to-no predictive validity in determining employee performance (Nielsen and Kuhn 2009). Additionally, an organization must have written consent of the candidate to obtain a credit report. As a result, unless the position has a direct relevance to financial responsibility, credit checks should be avoided as there are more valid, easier, and cost-effective tests that can be administered to measure these traits.

Criminal background checks exist in two forms: candidate self-report on an application and criminal history checks performed by a third party. The time frame for these checks can vary from having ever committed a crime to a crime in the past 5 years, as well as discerning the severity of the crime such as having been convicted of or plead guilty to a misdemeanor or a felony. In both self-report and third-party checks, 58% of organizations report providing candidates an opportunity to explain their conviction and why it should not affect the organizations' hiring decision. While this practice is not legally mandated, it is generally considered a "best practice" (Aamodt 2015). Another best practice is to refrain from performing any background check until a conditional job offer is made. This mitigates the adverse impact of the background check. Criminal history checks have a high predictive validity in determining person-organization fit factors such as conscientiousness and several counterproductive behaviors, despite having little validity in determining task performance (Aamodt 2015).

The social media "background check" is quickly becoming the third major category of candidate history evaluation with approximately

70% of employers using social media to recruit and/or screen candidates and 57% among these reporting that they have not hired someone due to inappropriate content on their profiles (Careerbuilder 2018). Social media sites such as Facebook allow organizations to quickly get an insight as to what type and quality of person a candidate may be, even allowing them to learn information about the candidate that may not have come up during an interview or other selection procedures. However, the information gleaned from this method is often more harmful than helpful. While organizations may feel more secure in their hiring decisions if they can infer judgment about a candidate's character from their social media profile, there is no empirical evidence that supports the validity and utility of this method. Use of social media as a tool to perform background checks only affects the perceived fit and provides no useful information in actually determining a candidate's organizational fit or job fit (Chiang and Suen 2015).

In addition to providing no benefit over existing methods, use of social media to perform background checks can also cause major risks to the organization. The first risk is that using social media as a selection test may reduce the perceived attractiveness of the organization as a potential employer to the candidate and may make a candidate less likely to accept a position (Drouin et al. 2015). The second, and potentially more serious risk, is that using social media as a selection tool can reveal protected information about the candidate, such as race, religion, or a disability, which may have otherwise never have been brought up. If an organization has access to this information, regardless of whether it actually influenced the hiring decision, it can lead to litigation against the organization for discrimination (Van Iddenkinge et al. 2016). This becomes risky as most people have such information publicly displayed on their social media profiles. Many organizations have circumvented this issue by utilizing third parties to screen a candidate's profile and only report back relevant information. However, the cost to do this often greatly outweighs the benefit of the information in the selection process.

Evaluating Selection Test Results

After an organization has determined which aspects of a position they wish to test for and which types of tests to use, developed or purchased those tests to measure the necessary employee qualities, and finally administered those tests, it can begin to analyze the results and find the best candidate for the position. Commonly used methods to make selection decisions include multiple-hurdle and multiple-regression. The process of multiple-hurdle selection involves administering each selection test one at a time, starting with the most cost-effective test first, and then evaluating the results of that test and eliminating candidates who did not pass before continuing on to the next most cost-effective test or hurdle. This process continues until all tests have been administered and a much smaller pool of candidates remain. In this process, it is important to determine a cutoff score for every given test. This cutoff score is the minimum score that can be considered passing. For security tests, this would likely involve a pass/fail decision based on the results of a background check.

In multiple regression, instead of using separate cutoff scores and eliminating candidates by using their scores on each test, a formula is used to create a composite score from each individual test score. This formula is usually generated by applying the selection tests to the current employees and examining their relationship with job performance levels. Then, the cutoff score is applied to this composite score. However, security tests would likely not be included in this formula and still be used on a pass/fail basis depending on the security needs of the organization and the requirements of the job. Both multiple hurdle and multiple regression have been shown to have utility in selection such that using such methods lead to higher scores in the criterion and significant monetary savings resulting from hiring better employees (Ock and Oswald 2018). Among the two methods, multiple-regression approach has been found to lead to higher levels of job performance. However, this does not always translate to bigger savings such that for lower level jobs, multiple-hurdle method was

found to lead to greater cost savings for the organization (Ock and Oswald 2018).

Conclusion

Personnel selection is a necessary process for all organizations, big or small, private or public. With a focus on security in the personnel selection process, this chapter presented the purpose, method, and benefits and drawbacks of the most common types of personnel selection and methods of evaluating those tests available to organizations. Using these evidence-based methods to make employee selections, especially by a security supervisor and for the role of security personnel, organizations are likely to see lower security risks and higher job performance. While there are a number of ways organizations can combine personnel selection tests, what is most important is that the organization achieves the goals it set out to do. With a focus on organizational security, an ideal personnel selection process would be using a security test administered by a security supervisor along with whichever selection tests best measure a candidate's person-organization fit and person-job fit for the specific position. The organization would then utilize the most appropriate analysis method in order to make their final selection decision.

Cross-References

- ▶ Physical Security: Best Practices
- ▶ Personnel Security: Recruitment
- ▶ Security Management

References

Aamodt, M. G. (2015). Using background checks in the employee selection process. In C. Hanvey & K. Sady (Eds.), *Practitioner's guide to legal issues in organizations*. New York: Springer.

CareerBuilder. (2018). *More than half of employers have found content on social media that has caused them not to hire a candidate.* Retrieved from http://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey

Chiang, J., & Suen, H. (2015). Self-presentation and hiring recommendations in online communities: Lessons from LinkedIn. *Computers in Human Behavior, 48*, 516–524.

Doverspike, D., & Arthur, W., Jr. (2012). The role of job analysis in test selection and development. In M. A. Wilson, W. Bennett Jr., S. G. Gibson, & G. M. Alliger (Eds.), *The handbook of work analysis: Methods, systems, applications and science of work measurement in organizations* (pp. 381–399). New York: Routledge/Taylor & Francis Group. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2011-29889-021&site=ehost-live&scope=site.

Drouin, M., O'Conner, K. W., Schmidt, G. B., & Miller, D. A. (2015). Facebook fired: Legal perspectives and young adults' opinions on the use of social media in hiring and firing decisions. *Computers in Human Behavior, 46*, 123–128.

Kristof, A. L. (1996). Person-organization fit: An integrative review of its conceptualizations, measurement, and implications. *Personnel Psychology, 49*(1), 1–49. https://doi.org/10.1111/j.1744-6570.1996.tb01790.x.

Kristof-Brown, A., & Guay, R. P. (2011). Person-environment fit. In S. Zedeck (Ed.), *APA handbooks in psychology. APA handbook of industrial and organizational psychology, Vol. 3. Maintaining, expanding, and contracting the organization* (pp. 3–50). Washington, DC: American Psychological Association. https://doi.org/10.1037/12171-001.

Marcus, B., Taylor, O. A., Hastings, S. E., Sturm, A., & Weigelt, O. (2016). The structure of counterproductive work behavior: A review, a structural meta-analysis, and a primary study. *Journal of Management, 42*(1), 203–233.

National Center for O*NET Development. (2018). 11-9199.07 – Security Managers. *O*NET OnLine*. Retrieved from https://www.onetonline.org/link/summary/11-9199.07.

National Center for O*NET Development. (2019a). 15-1122.00 – Information Security Analysts. *O*NET OnLine*. Retrieved from https://www.onetonline.org/link/summary/15-1122.00.

National Center for O*NET Development. (2019b). 33-9032.00 – Security Guards. *O*NET OnLine*. Retrieved from https://www.onetonline.org/link/summary/33-9032.00.

Nielsen, M. L., & Kuhn, K. M. (2009). Late payments and leery applicants: Credit checks as a selection test. *Employee Responsibilities and Rights Journal, 21*(2), 115–130. https://doi-org.proxy006.nclive.org/10.1007/s10672-008-9071-5.

Ock, J., & Oswald, F. L. (2018). The utility of personnel selection decisions: Comparing compensatory and multiple-hurdle selection models. *Journal of Personnel Psychology, 17*(4), 172–182. https://doi-org.proxy006.nclive.org/10.1027/1866-5888/a000205.

Ones, D. S., Viswesvaran, C., & Schmidt, F. L. (2012). Integrity tests predict counterproductive work behaviors and job performance well: Comment on Van Iddekinge, Roth, Raymark, and Odle-Dusseau (2012). *Journal of Applied Psychology, 97*(3), 537–542. https://doi-org.proxy006.nclive.org/10.1037/a0024825.

Oostrom, J. K., & De Soete, B. (2016). Ethnic differences in perceptions of cognitive ability tests: The explanatory role of self-serving attributions. *International Journal of Selection and Assessment, 24*(1), 14–23. https://doi.org/10.1111/ijsa.12125.

Sebanz, N., & Shiffrar, M. (2009). Detecting deception in a bluffing body: The role of expertise. *Psychonomic Bulletin & Review, 16*(1), 170–175. https://doi.org/10.3758/PBR.16.1.170.

Spector, P. E. (2012). *Industrial and organizational psychology: Research and practice*. Oxford: Wiley.

Sydell, E. J. (n.d.). Making decisions about people. Retrieved from https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/pages/sydell_makingdecisionsaboutpeople.aspx

Thornton, G. C., III, & Kedharnath, U. (2013). Work sample tests. In K. F. Geisinger, B. A. Bracken, J. F. Carlson, J.-I. C. Hansen, N. R. Kuncel, S. P. Reise, & M. C. Rodriguez (Eds.), *APA handbook of testing and assessment in psychology, Vol. 1: Test theory and testing and assessment in industrial and organizational psychology* (pp. 533–550). Washington, DC: American Psychological Association. https://doi.org/10.1037/14047-029.

U.S. Office of Personnel Management. (2019a). Assessment & selection: other assessment methods. Retrieved from https://www.opm.gov/policy-data-oversight/assessment-and-selection/other-assessment-methods/integrityhonesty-tests/

U.S. Office of Personnel Management. (2019b). Assessment & selection other assessment methods. Retrieved from https://www.opm.gov/policy-data-oversight/asse ssment-and-selection/other-assessment-methods/struct ured-interviews/

Van Iddenkinge, C. H., Lanivich, S. E., Roth, P. L., & Junco, E. (2016). Social media for selection? Validity and adverse impact potential of a Facebook-based assessment. *Journal of Management, 42*, 1811–1835.

van Zyl, C. J. J., & de Bruin, G. P. (2018). Predicting counterproductive work behavior with narrow personality traits: A nuanced examination using quantile regression. *Personality and Individual Differences, 131*, 45–50. https://doi.org/10.1016/j.paid.2018.04.014.

Further Reading

Doverspike, D., & Arthur Jr, W. (2012). The role of job analysis in test selection and development (pp. 381–400). New York, NY: Routledge.

Schmitt, N. (Ed.). (2012). The Oxford handbook of personnel assessment and selection. OUP USA.

Outtz, J. L. (2010). Adverse impact: Implications for organizational staffing and high stakes selection. (J. L. Outtz, Ed.). New York, NY: Routledge/Taylor & Francis Group.

Personnel Security: Training

Jamie Sanderson Reid
Thomson Reuters, Richmond, VA, USA

Keywords

Personnel security · Training · Education · Awareness

Definition

Personnel security training refers to provision of "awareness, knowledge, understanding, and skills needed by any person with the responsibility and authority to perform tasks" (ASIS 2012a, p. 63), which develop and maintain behaviors and competency required for the organization to reach its security program goals.

Introduction

Effective utilization of personnel security as a security countermeasure (Sennewald 2011) requires an organization to "retain and train personnel with the skill, knowledge and ability" to meet its security requirements (ASIS 2012a, p. 59). Training typically has two main foci. First, the organization must determine specific behaviors that facilitate goal achievement, as well as identify behaviors that interfere or interrupt accomplishing these goals (Knowles 1973, p. 129). Second, training aims to improve job performance and thus will include the modification of current behaviors and development of new behaviors that serve that purpose (Nadles 1970, pp. 40–41 in Knowles 1973, p. 98).

According to Physical Asset Protection Standard, "personnel play the most significant part in the success of a security program" (ASIS

2012b, p. 50). Personnel classifications can include visitors, tenants, employees, service providers, and security professionals (ASIS 2012b). The focus of training for general employees is predominantly on security awareness, personnel at every level are involved in some way with the security program and thus require training to achieve security program goals (ASIS 2012b). Security professionals who implement asset protection measures range from security officers to managers, and these individuals require security skills, knowledge, and understanding that provide competencies required in the security profession (ASIS 2012b).

Within the workplace, training is aimed at improving performance through developing competencies or aligning behaviors with the identified requirements of the role. ISO 19011 defines competence as the "ability to apply knowledge and skills to achieve intended results." According to ASIS (2012a) "personnel, competence, and training needs are an output of the context of the organization and its contractual requirements, as well as the risk assessment and definition of objectives" (p. 59). The organization is responsible for identifying training needs and ensuring that all personnel including employees, subcontractors, and other stakeholders are sufficiently trained (ASIS 2012a). The aim of security education, therefore, is "to enable people in our organization to carry out their roles in our security program effectively and reliably" (Roper et al. 2006, p. 2). This entry provides a holistic view of personnel security training including frameworks for training development, relevant topics, and adult learner considerations that support effective learning.

Personnel Security Training

The organization's key groups of personnel requiring security training are general employees and security professionals responsible for implementation of asset protection. Additionally, visitors and third parties may require training. The organization must also consider legal and regulatory requirements which include specifications for personnel security training. There is a common saying that people are the weakest link in a security program, because the effectiveness of administrative and technical controls is limited by the implementation and operation of controls by people. Personnel security, which aims to leverage the human aspects in security countermeasures, is built on the foundation of training as a means to achieve required security performance objectives through personnel. General employees require an understanding of security policies and procedures which they must follow for the organization to achieve security program goals. Security professionals, in contrast, require job-related skills and competencies necessary to implement the asset protection program.

Training for General Employees

Training for general employees provides skills, knowledge, and information to enable understanding of security policies and promotes behaviors that conform to the policies. General employees often have limited background and interests in security.

The Skills, Knowledge, and Information (SKI) methodology presented by Roper et al. (2006) provides a threefold approach to security education, awareness, and training that includes skill, information, and knowledge which are useful for clarifying objectives of security training. According to this method:

- A skill is an ability, usually developed through practice.
- Information is something that can be known: facts, steps in a procedure, and conditions that signal the need for something to be done.
- Knowledge is information that is stored in a performer's brain so he or she can take it out and use it when needed (Roper et al. 2006, pp. 33–34).

Roper et al. (2006) recommend the security educator design training to meet the employees' needs by groups or profiles according to assigned job functions. Often training is the preferred approach to directing and aligning behaviors that

impact security requirements for an organization as noted by Roper, Grau, and Fischer (2006 p36): "The traditional approach to handling a Skills, Knowledge, and Information (SKI) problem is training." Skills, Knowledge, and Information (SKI) provides a focused approach to defining training requirements in terms of skills, knowledge, and information. The Skills, Knowledge, and Information (SKI) method is particularly useful when designing security compliance training for general employees.

A business' ability to meet legal, regulatory, and compliance requirements is one of the most compelling reasons for providing security training to general employees. The main goal of security compliance training is typically to meet and maintain compliance requirements. Puhakainen and Siponen (2010) highlight research findings in the areas of security training and employee compliance including the following considerations which impact the effectiveness of employees' compliance through training. Their seven practical implications are summarized in Table 1. For this type of training to also provide benefits to the organization, the program should be integrated with day-to-day business communications and processes, be continuous, and have top management support. For learners to engage with the material in a meaningful way that can promote appropriate security behaviors, the training should be relevant, facilitate discussion, and consider learners' previous knowledge. The adult learning considerations discussed later will provide more insights as to why it is important to engage adult learners in this way and some suggestions on how to foster a learning environment conducive to adult learners.

Personnel Security: Training, Table 1 Seven practical implications for security compliance training

Organization elements required for successful training program	Use a systematic and continuous training program
	Integrate with normal business communication efforts to integrate security with day-to-day business processes
	Ensure visible support by top management
Training elements required for the training program to effectively engage learners	Take into account the learners' previous knowledge as captured through surveys or interviews
	Include learning tasks that demonstrate personal relevance to the learners
	Use training methods that enable learners' cognitive processing by incorporating cause-and-effect models
	Facilitate employee discussion through educational sessions and active participation in monitoring and reporting of security program status

Training for Security Professionals

Security professionals are employees who directly support implementation of the asset protection program. Security officers carry out specific tasks within the security program, which are documented within the standard operating procedures or post orders. The security supervisor is responsible for overseeing security officers, including their quality control responsibilities. The security manager is responsible for keeping the security program running efficiently and provides direct supervision over the supervisor and officers. The security manager requires not only technical security knowledge but also supervision and management training.

Security officer training is aimed at ensuring individuals have the requisite technical security skills and competencies to carry out standard operating procedures and post orders in addition to generally supporting the objectives of the security program. Pre-assignment, on-the-job, and annual training is recommended for private security officers (ASIS 2010). The Private Security Officer Selection and Training Guideline from ASIS (2010) provides a list of 17 minimum training topics (ASIS 2010, pp. 9–10):

1. Nature and Role of Private Security Officers
2. Observation and Incident Reporting

3. Principles of Communication
4. Principles of Access Control
5. Principles of Safeguarding Information
6. Emergency Response Procedures
7. Life Safety Awareness
8. Job Assignment and Post Orders
9. Employer Orientation and Policies
10. Workplace Violence
11. Conflict Resolution Awareness
12. Traffic Control and Parking Lot Security
13. Crowd Control
14. Procedures for First Aid, Cardiopulmonary Resuscitation, and Automated External Defibrillators
15. Crisis Management
16. Labor Relations
17. Basic Computer Skills

The training topics identified by ASIS include skills typically required by security officers in the conduct of their job. Additional topics may be required depending on the industry and environment where the security professional performs their duties. It is further recommended that "defined training objectives should be based on the risk assessment and facilitate uniformity and standardization of training requirements" (ASIS 2012a, p. 63).

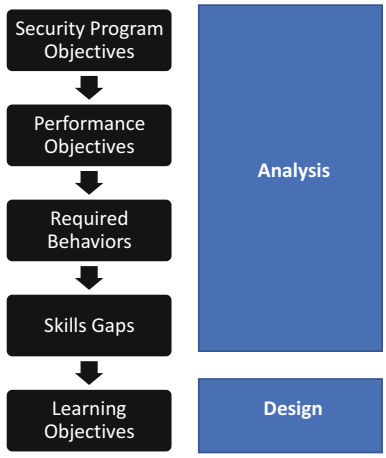
Developing Security Training Programs with ADDIE

Personnel security training should be developed based on best practices in instructional design. Training is developed to address a specific need. The ADDIE instructional design process is a generally accepted approach to instructional design which supports design and delivery of training targeted at diagnosed needs. ADDIE includes the five phases of analysis, design, development, implementation, and evaluation (Chevalier 2011; Peterson 2003). Understanding the ADDIE process can aid training developers in creating an effective security training program. Table 2 summarizes each ADDIE phase and outcome. Analysis involves diagnosing the learning need. In design, the instructional strategy and course outline are created to achieve the learning need. Development is the process of piloting and creating the actual course materials. In implementation, the training is actually delivered via various methods. There are several different approaches and delivery methods including face-to-face learning, online asynchronous and synchronous learning, and videos. The approaches will be determined during the design phase, and training is delivered via the method in implementation. Pros and cons associated with each of the approaches are discussed further in the section on implementation. Finally, in evaluation, feedback to enable continuous improvement is collected from participants.

Personnel Security: Training, Table 2 ADDIE phase outcomes

ADDIE phases	Outcomes
Analysis	Identification of knowledge, skills, and attitudes necessary, training needs matrix, training needs assessment, gap analysis,
Design	Instructional strategy, knowledge-based outcomes, content outline
Development	Training materials
Implementation	Delivery of training materials
Evaluation	Surveys, performance improvement metrics, formative and summative evaluation

Analysis. Analysis requires examination of learning needs in terms of standards and competencies (Peterson 2003). The training need analysis considers training requirements and enables development of the course content. Analysis should be open-ended, considering all possible root causes of the performance gaps, and aligned with human performance training (HPT) ideology. HPT does not presuppose training as the only intervention but considers other non-training interventions that could achieve the required on-the-job behaviors (Abaci and Pershing 2017). The outcome of the analysis phase is clarification of requirements in the training need assessment or gap analysis report. Figure 1 provides an adaptation of Bersin's (2004) approach to aligning training with business needs, simplified with a focus on deriving personnel security



Personnel Security: Training, Fig. 1 Development of learning objectives

learning objectives from the security program objectives.

Design. The outcome of the design phase is content outline, instructional strategies, learning activities, methods, and media which will be used to address the knowledge, skill, and attitude gaps identified in analysis (Chevalier 2011). The learning objectives – "description of a behavior, performance, or skill learners should be able to exhibit following a course or other learning intervention" – are decided based on consideration of skills and knowledge required to perform behaviors (Bersin 2004, p. 28). The course objectives "should be specific and measurable" and become the "landmarks by which you guide the class" (Spalding 2014, p. 40). In this phase decisions are made for the course including instructional, visual, and technical design strategies. The design phase involves planning the schedule of learning which includes determination of the general approach, what will be learned and how much of the material can be covered, and determining how the participants will engage with the material (Rogers and Horrocks 2010, p. 251). Based on the learning objectives and constraints, decisions on the most appropriate methods for learning should be determined based on the course need to employ the following four main categories:

- Presentation methods
- Participatory methods
- Discovery methods
- Evaluator methods (Rogers and Horrocks 2010, p. 253)

Presentation methods include demonstrative teaching activities, participatory methods include interactions between teacher and learners, discovery methods include student learners discovering on their own such as through reading, and evaluator methods are used to evaluate learning such as tests or quizzes (Rogers and Horrocks 2010, p. 253).

Development. The development phase utilizes the outcomes of the analysis and design phases to create training materials, media, and training manuals (Chevalier 2011). Course materials should be developed to elicit appropriate levels of the four phases of learning:

- Activity – doing something
- Reflection – thinking about the experience
- Theory – seeing where it fits in with theoretical ideas
- Pragmatism – applying the learning to actual problems (Rogers 2007, p. 26).

Once materials are drafted, they should be shared with representatives of the target audience for piloting. Feedback from piloting can then be incorporated in the final version of training materials.

Implementation. Implementation involves the delivering of training and providing of appropriate work environment and resources to apply the learnings (Chevalier 2011). There are many methods and media available for delivery of training including the most common approaches of face-to-face classroom, virtual live online classroom, and self-paced online classroom. The decision on approach and methods is determined in the design phase. In implementation the students will engage with the determined methods and media. Bersin (2004) provides a list of various methods and media which may be combined for the delivery of training, and, while the technology continuously evolves, the concepts and approaches remain relevant. In addition to the classroom spaces organized and

controlled physically and virtually by the instructor, global communities of practice are an emerging expansion of learning environments. These communities have been empowered by the ubiquity of mobile technology and "integration of cognitive and social aspects of learning" in the workplace and daily life (Liu 2018, p. 2). Social learning may be facilitated in an organized way through collaboration and hands-on learning formally arranged in online learning spaces (Liu 2018). Informal communities also evolve through professional organizations and other groups that leverage online collaboration platforms. A few of the most relevant methods discussed by Bersin and Liu (2018) are summarized in Table 3, categorized by high-level learning objectives.

There are pros and cons of each delivery method. According to Bersin (2004), when to use the various media types is an important question. Live events whether in-person instructor-led or live e-learning events are more costly however deliver benefits of connections between the learners and instructor. In particular instructor-led training is helpful when:

- Learners are being introduced to brand new material and have no prior experience with the topics.
- Culture building needs are high.
- Direct interaction and discussion with peers and discussion are primary to the learning process (Bersin 2004, p. 145).

Personnel Security: Training, Table 3 High-level learning objectives for the three teaching methods

Gain awareness	Acquire knowledge	Build skill
Webinars Video Blog	E-learning (synchronous, live events, and asynchronous, self-study) Instructor-led training Interactive webinars Written projects	Simulations Service-learning projects Field study projects Game-based learning projects Instructor-led training

The key elements which must be balanced across the different methods are interactivity, cost, and scalability. Instructor-led events are expensive but provide more support to the learner. E-learning is generally more scalable and less interactive unless delivered to small groups and requires some logistical considerations including scheduling and technology access. Simulations and game-based learning require more expertise in the development phase; however it can be scalable and very effective for transferring skills.

Evaluation. Evaluation is used to determine whether the training delivered made the impact intended in terms of achieving the desired outcomes through participants applying learnings and demonstrable changes in behavior (Chevalier 2011). Kirkpatrick's four levels of evaluation is a well-known system of learning evaluation which includes the four steps of reaction evaluation, learning evaluation, behavior evaluation, and result evaluation. Evaluation may include post-training surveys, metrics on performance improvement, and other methods that document the impact training has made on meeting the training needs (Chevalier 2011). The training need assessment in the analysis phase identified requirements, and evaluation validates if those requirements have been met through the implementation of training. The feedback from evaluation should be used for continuous improvement in the training cycle by updating training materials and delivery methods where necessary.

Adult Learning Considerations

Development of personnel security training should include consideration of a best practice for adult learning. The trainer or facilitator is responsible for providing an environment conducive to learning, which includes the space and resources that enable achievement of the learning objectives.

Adult education is not only a means for the organization to achieve its goals through developing competencies of individuals, it also provides personnel the opportunity for self-actualization

through development of competencies which support growth (Knowles 1973). A teaching model is recommended that leverages prior experience, personal motivation, and the problem-centered orientation. Teachers of adults should have attitudes towards the student learners and subject matter which include flexibility and enthusiasm. "Planning skills, communication skills, caring-guidance skills, evaluation skills, and subject skills" must be deployed effectively with an understanding of the philosophy of adult teaching to effectively reach adult learners (Rogers and Horrocks 2010, p. 260). One way to achieve this balance is through teachable moments which provide opportunities for participants to "use their existing experience and knowledge; exercise their learning abilities; and practice" (Rogers and Horrocks 2010, p. 249).

"The best-designed adult learning aims to minimize the disadvantages and maximize the advantages of the experience adults bring with them to learning" (Rogers 2007, p. 35). Current research also supports the need for effective learning to extend beyond dissemination of content knowledge to learning facilitated by "social, cultural, and historical contexts" (Liu 2018). This requires a greater effort on the course developer and facilitators to provide physical or virtual space for positive interaction between participants. In addition to interaction, scenario-based learning is particularly helpful for security professionals. Existing security standards for training recommend practical training including scenario-driven training that models potential conditions security personnel may face in the performance of their job (ASIS 2012a). Developers of security personnel training programs can optimize the learning experience for participants by designing in alignment with adult learning models, while encouraging social learning and scenario-based learning which together support sharing experience and problem solving.

Conclusion

Training is a critical element of personnel security. Providing training for personnel who hold security responsibility and accountability ranging from policy compliance to asset protection develops the competencies, knowledge, behaviors, and attitudes required to meet the organization's security objectives. Personnel security training can leverage current technology to provide multiple methods and media for delivery of training content. Designing training that is relevant for practical situations the learner will encounter with a problem-solving approach is a key requirement whether the target training audience is general employees or security professionals.

In most cases, training for general employees is required annually to meet compliance requirements. This often takes the form of a self-paced online course which is completed along with an end of course test delivered via a corporate learning management system. All employees are required to participate annually particularly for information security courses. Another common approach is to include security training in the overall new employee orientation training. Both of these approaches will require collaboration with the human resources or training department responsible for the learning management system and new employee orientation training. The security manager can also provide general awareness training by departments through arranging with department managers to have security briefings as part of department meetings on an annual or quarterly basis. This approach enables the facilitator to focus on the specific concerns and requirements of the department to make the experience more relevant.

There are several options for security personnel training offered by security professional associations, colleges, and universities. Some states require security guards to be licensed, and those states do have varying requirements for licensing which may include completion of a state-certified training. For those seeking to build a career in security, professional certification is a popular approach as the process to attain certification is rigorous including exams and experience reviews that demonstrate proficiency in the body of knowledge. Many job postings request or require that security professionals have security certifications. ASIS International offers a suite of certifications for security professionals with a range of

focus areas and experience requirements up to and including security management. The International Foundation for Protection Officers offers certifications for protection officers and supervisors.

The security professional often has a critical role in the design and delivery of personnel security training. Depending on resources available, the security professional may even have full responsibility for security training. Even in cases where the security professional is supported by an instructional designer for development of personnel security training, it is important for the security professional to have a basic understanding of instructional design principles such as the ADDIE process and a firm understanding of security program objectives and how they relate to performance objectives and behaviors required. Moreover, the security program objectives must align with the organizational objectives. Where possible it is best to seek support and collaborate with the human resource department to leverage existing expertise and resources for training. The security professional should leverage existing methods of communication in the organization through ongoing collaboration and relationship building with human resources, corporate communications, department managers, and all other relevant stakeholders who can support the program for personnel security training. The personnel security training approach should be integrated into holistic improvement efforts for maximum effectiveness.

Cross-References

- ▶ Personnel Security: Hiring
- ▶ Personnel Security: Retention
- ▶ Security Guards: Academic and Training Programs
- ▶ Security Management

References

Abaci, S., & Pershing, J. (2017). *Research and theory as necessary tools for organizational training and performance improvement practitioners.* TechTrends. 61, 19–25. https://doi.org/10.1007/s11528-016-0123-7.

ASIS. (2012a). *Management system for quality private security company operations – Requirements with guidance* (ANSI/ASIS PSC.1-2012). Alexandria: ASIS International/American National Standards Institute.

ASIS. (2012b). *Security Management Standard: Physical Asset Protection. American National Standard*. Alexandria: ASIS International/American National Standards Institute.

ASIS International. (2010). *Private security officer selection and training guideline*. Alexandria: ASIS International.

Bersin, J. (2004). *The blended learning book: Best practices, proven methodologies and lessons learned*. San Francisco: Wiley.

Chevalier, R. (2011). When did ADDIE become addie? *Performance Improvement, 50*(6), 10–14.

Knowles, M. (1973). *The adult learner: A neglected species*. Madison: American Society for Training and Development.

Liu, J. C. (2018). Design of innovative learning environment: An activity system perspective. In *Learning, design, and technology* (pp. 1–25). Springer, Cham.

Peterson, C. (2003). Bringing ADDIE to life: Instructional design at its best. *Journal of Educational and Hypermedia, 12*(3), 227.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778.

Rogers, J. (2007). *Adults learning*. Maidenhead: McGraw-Hill Education.

Rogers, A., & Horrocks, N. (2010). *Teaching adults*. Maidenhead: McGraw-Hill Education.

Roper, C., Grau, J., & Fischer, L. (2006). *Security education, awareness and training*. Burlington: Elsevier Butterworth-Heinemann.

Sennewald, C. (2011). *Effective security management* (5th ed.). Burlington: Butterworth-Heinemann.

Spalding, D. (2014). *How to teach adults: Plan your class, teach your students, change the world*. Hoboken: John Wiley & Sons.

Further Reading

Brislin, R. (2014). *The effective security officer's training manual* (3rd ed.). Waltham: Butterworth-Heinemann.

Carpenter, P. (2019). *Transformational security awareness: What neuroscientists, storytellers, and marketers teach us about driving secure behaviors*. Indianapolis: Wiley.

Fischer, R., Halibozek, E., & Walters, D. (2012). *Introduction to security* (9th ed.). Waltham: Butterworth-Heinemann.

Nadler, L. (1970). Developing Human Resources. Houston: Gulf.

Silberman, M. (2006). *Active training: A handbook of techniques, design, case examples, and tips*. San Francisco: Wiley.

Physical Security: Best Practices

Michael P. Coole and David J. Brooks
Security Science, School of Science, Edith Cowan University, Perth, WA, Australia

Keywords
System · Control · Diagnose · Inference · Treatment · Professional · Security zones

Definition

Best practice in physical security is the professional use of a systems approach, comprising accurate threat and risk assessments (diagnosis), an aligned protection strategy based on sound theory and security principles (inference), and a mitigation system (treatment) that fulfils operational requirements accordant with legislation, standards, and engineering practice to manage the protection of assets, information, and personnel from damage, loss, or unauthorized access against internal and external threats.

Introduction

It is the duty, as a standard of care, for professionals to exercise diligence in their application of standardized expertise when carrying out work, where professional competence (duty) is judged against the state of knowledge that exists in the form of published methodologies, standards, codes, and research. Consequently, professionals should exercise their professional duty accordant with best practice in order to meet their duty of care obligations in the professional setting.

In considering the public and organizational duty to protect in a professional undertaking, the broad practice of physical security is what many citizens perceive when they consider or pursue day-to-day safety or security, being protected from harm or loss. Physical security includes engineered elements across the built environment that are designed to reduce threats or risks by controlling and managing spatial movement (Parker 2007, p. 233). Therefore, physical security aims to direct environmental control or influence over a defined space. For example, physical security includes protection of the grounds surrounding a facility, and its interior and contents (Fischer et al. 2008). Such control is achieved through the process of layers of physical manipulation measures to mitigate against threats or environmental design facets to reduce opportunistic deviance.

Given the broad usage and associated depth and complexity of physical security's knowledge basis, it is problematic within the scope of this entry to singularly state what constitutes physical security best practices. Consequently, the entry submits that the best practices in physical security must be grounded in the professional application of a defined body of knowledge. All professionals are required to exercise the skill of an ordinary person within their profession when carrying out work. That is, they are bound to exercise due care, expertise, and diligence (Zipser 1999). The professional is deemed to hold both the knowledge (academic basis) and competence to use held knowledge in accordance with the average field practitioner. Competence is judged against the state of knowledge that exists at the time, recognizing that professional bodies of knowledge continue to advance. As Zipser stated, "the professional should be aware of developments which have entered the general corpus of knowledge relevant to their field" (Zipser 1999, p. 4).

Such competence is demonstrated through the conformity to common practice or norms encapsulated within the defined body of knowledge including where available, research findings, published codes, and standards. As such, the inclusive body of knowledge provides a platform for understanding best practice in physical security. A codified body of knowledge has been established for physical security (See Coole et al. 2018). Such codification had synergies with engineering and embodied a matrix of knowledge categories organized accordant to professional practice modalities, including *diagnosing* the security problem, *inference* to reach the optimal

Physical Security: Best Practices, Table 1 Modalities of physical security practice

Modality	Intent	Professional knowledge	Tools
Diagnose	Identify and articulate the problem/s	Criminology theories Security risk Communication	Threat assessment Criticality/Impact assessment Vulnerability assessment Risk assessment Risk context statement
Inference	Defining a mitigation solution from many options in articulating the Security Strategy	Crime prevention Systems theory Defense in depth Deter, detect, delay and response (D3R) Protection in depth CPTED	Situational crime prevention Codes and standards Policy Guidance documents Operational objectives
Treatment	Design, apply and maintain the physical Security Strategy	Physical security Control Response Engineering design	Technical specifications Intrusion detection Barriers and control portals Response procedures System modelling

mitigation among many options, and finally, implementation of *treatment*. Therefore, the entry presents the notion of best practice in physical security through the modalities of a *practice* model. Such a model aligns the body of corpus in which professional duty is judged against the physical security professional tasks of diagnosis, inference, and treatment.

Structure and Application of Physical Security's Knowledge

Best practice in physical security must align with the notion of best practice across other professional disciplines. The modalities model of practice embodying diagnosis, inference, and treatment elements of practice transcend all disciplines and represent a problem focused structure to professional practice (Abbott 1988). Garcia (2008, p. xvii) acknowledged physical security as a problem-centered approach in which understanding and defining the security problem occurs prior to designing and evaluating a protective mitigation system. As Sennewald stated, "security professionals engage in a problem solving process, in which the consultant must first identify the problem(s), gather available data pertaining to the problem(s), analyse that data, and then offer advice in the form of recommendations that will solve, cure, or otherwise minimize the problem(s)" (Sennewald 2013, p. 7). Consequently, the modalities of practice shown in Table 1 represent the most appropriate framework for denoting physical security best practice.

Physical Security Diagnosis – The Problem

Diagnosis is defined as the cognitive task associated with assembling a client's needs (Abbott 1988) or articulating the problem. The body of knowledge associated with diagnosis facilitates establishing the physical protection security threat and risk context. Establishing context has always been an initial component of risk management and includes both internal and external operating context. Context also includes defining the legal context, which outlines required and acceptable behaviors and sets standards. Consequently, in the application of physical security, there are three salient environmental contexts to consider in problem diagnosis:

- Regulatory environment – rules defined and controls directed by a body
- Advisory environment – controls advised
- Self-driven security environment – an industry or organization sets its own risk appetite

Security Risk Management

The professional task of diagnosis is undertaken as security risk management (see ▶ "Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats" entries in this encyclopedia), an underpinning activity for all security practice (Talbot and Jakeman 2009; Smith and Brooks 2013). Security risk management incorporates data generated from asset identification and evaluation, threat assessment, security survey and vulnerability assessments, and risk assessment. Consequently, for security to be effective, it must target defined threats.

Informing threat are the theories of Routine Activity, Crime Pattern, and Rational Choice (see ▶ "Security: Theories" entry in this encyclopedia). Routine Activity highlights how movement and activities of both potential offenders and victims relate to targets, motivated offenders, and an absence of guardians interact with intent and capability. Crime Pattern theory highlights the notion that crime fits patterns which can be understood (Lab 2014). Rational Choice theory, as risk management, is predicated on altering the cost benefit analysis of a rationally adversary (Clarke 1980).

For diagnosis, data is analyzed through the process of Security Risk Management, using assessment Standards (ISO 31000 2018; Risk Assessment ANSI/ASIS/RIMS RA-12015) or guidelines (Standards Australia ASHB167 2006). Such instruments are an aide memoire to ensure assessors consider all facts in a logical process; however, they do have limitations including likelihood ratings that are based on averages and biased by perception of probabilities, and consequences remain an estimated variable.

The art of diagnosis therefore lies in defining the real issue (problem). Consequently, best practice in physical security requires a thorough and documented diagnosis of the security risk problem, undertaken to ensure sound strategy can be directly aligned to threat and risk drivers. Diagnosis is communicated, usually in report format, which go by many names including *risk context statement*, detailing the key assets at risk, threat drivers, their consequential risk, and business case to protect, designating contextual degree of protection. Therefore, diagnosis is a clinical judgment that is guided by the presence and relevance of risk factors, historical, clinical, and potential management influences.

Physical Security Inference – The Security Strategy

Inference is focused towards establishing the functions of the protection plan (ASIS International's Physical Security Principles 2015). Professional inference, as a process, may be achieved through excluding what has failed (exclusion) or constructing threat scenarios (construction) relevant to defined threat actors, aligning the mitigation body of knowledge into a systematic strategy. Inference aims to set the security strategy (approach) and operational objectives.

The modality of inference is the use of fused knowledge of security and crime prevention theories and principles along with relevant codes, standards, and guidelines that facilitate the conceptual mitigation of the security problem. The functions of physical security is defined as controlling space, which includes delay, observing an area, situation or event, detecting events, and having an appropriate response to situations. Consequently, it is through the process of professional inference that sound theory and best practice is further layered into physical security best practice.

Function and Components of Physical Security

Situational Crime Prevention. Sound theory embodies numerous theoretical frames including Situational Crime Prevention (SCP), a crime prevention framework of preemptive measures in asset protection. SCP recognizes offenders' cost benefit choices and decisions in offending and presents a rubric of mitigation techniques. These include the objectives of increasing the effort to offend, increase the risks for offenders or reduce their rewards for offending. Such objectives are braced by prevention measures directed at highly specific forms of crime and involve the management, design, and manipulation of the immediate environment in a systematic and permanent way.

Systems Theory. Noting Situational Crime Prevention includes the systematic manipulation

of the physical environment to achieve protection identifies another core theory of physical security, namely, Systems theory. Systems theory is salient within the physical security literature and therefore, of significance for defining best practice. As Underwood (1984, p. x) expressed, security should be designed, implemented, and managed as a system. Such thinking is based on Bertalanffy's (1950) General Systems Theory, which premised that "there are principles which apply to systems in general, whatever the nature of their component elements, or of the relations or forces between them" (p. 139).

Within the physical security context, Garcia (2008) defined a system as an integrated collection of components or elements designed to achieve an objective according to plan. For example, the systematic plan for physical security is to interrupt and, where necessary, neutralize a malevolent adversary before they achieve their goal (Garcia 2008). Consequently, best practice embeds the principles of Systems theory into the protection solution.

Crime Prevention through Environmental Design. The systematic approach to physical security is also embedded into the theory of Crime Prevention through Environmental Design (CPTED). CPTED seeks to extend the notion of controlling people's behavior through natural environmental design and management. The premise draws from both social and physical sciences (American Institute of Architects 2003, p. 40) and is a well-established framework for embedding security strategy into environmental architecture.

Jacobs (1961) contended surveillance provided by legitimate users facilitates the keeping of the peace based on an intricate, almost unconscious, interaction of voluntary and enforced controls and standards by the people themselves. Jacobs coined *Eyes on the Street* to achieve such surveillance. Later, Newman (1972) argued that residential environments can inhibit crime by creating the physical expression of a social fabric that defends itself. Newman (1972, p. 3) defined defensible space as a surrogate term for the range of mechanisms, real and symbolic barriers, strongly defined areas of influence, and improved opportunities for surveillance that combine to bring an environment under control of its residence.

Contemporary CPTED aims to achieve security through reducing opportunities for individuals to successfully engage in deviant behavior (Fennelly and Crowe 2013). CPTED aids the security strategy through using natural surveillance, natural access control, and territorial reinforcement measures, coupled with image maintenance to maintain an expression of defended space. These overlapping and interrelated concepts employ physical and spatial factors, including situational and architectural strategies to ensure environmental context is designed to deter crime while supporting the intended purpose of a space. In many town planning environments, CPTED is captured in jurisdictional Planning Codes and guidelines, and best practice in physical security embeds this theoretical framework into the physical security strategy.

Defense in Depth. Defense in Depth aims to link physical security's functions and elements into a layered protection system to achieve security through interrelating people, technology, barriers, and procedures to achieve a robust physical security system (Smith 2003, p. 8). Such a strategy has been applied to the protection of assets for centuries, based on the argument that a protected asset should be enclosed by a succession of barriers. These barriers restrict unauthorized access to provide time for an appropriate response and recovery (Smith 2003, p. 8). The functions of Defense in Depth elements are:

- Deterrence – psychological measures to deter offenders from deviant acts
- Detection – means to alert that an unauthorized access is underway
- Delay – physical means to retard progress of an unauthorized access
- Response – means of interrupting and neutralizing an unauthorized access
- Recovery – planned approach to reactivating during or after a realized event to return to a priori state

The Systems approach to Defense in Depth interrelates the functions of detect, delay, and

response into an effective security system, referred to as a Physical Protection System (Garcia 2008).

Best practice also embeds well-established physical security principles. For instance, not all areas or protective contexts require the same level of physical security or complexity of system integration. Consequently, physical security strategy requirements are compartmentalized, based on the demarcation and division of space accordant with risk, generally referred to as *security zoning*. Security zoning holds that different levels of protective elements should be concentrated accordant with a cost benefit analysis based on risk. Diagnosis bounds the security assessment and such bounding is used to articulate the environmental limitations of the protection program, setting security zone that focuses the security strategy.

Balanced Protection. Best practice also embeds the principle of layers into the security strategy and includes *protection in depth* within Defense in Depth. This approach includes layering distinct security measures an adversary must defeat in sequence and considers the avoidance of single point failure in any protection plan (American Institute of Architects 2004, p. 11; Garcia 2008, p. 6; Williams 1981, p. 143), considered the "rings of protection" (Higgins 1989, p. 229).

Protection in depth incorporates the design philosophy of multiple detection, delay, and response capabilities (Williams 1981, p. 143; Garcia 2008, p. 6) that complement each other at each layer. Such an approach overcomes individual weaknesses and minimizes the consequences of individual component failure (Garcia 2008, pp. 5–6). The aim is to achieve what Wyss (2009) termed *balanced protection*, achieved when every scenario pathway into a protection environment presents the same level of difficulty.

Best practice within inference refers to setting the protection strategy and supporting operational objectives for the physical plan to achieve, documented as the security management plan. Such a plan is informed by the security risk context and directs the final design and commissioning of the physical security system and program. The security plan establishes the security zones and develops protection objectives to achieve a best practice principles framework within physical security's body of knowledge.

Physical Security Treatment

Treatment constitutes how the security strategy is functionally achieved through the commissioned components of the physical system. Treatment functionally achieves the elements of Defense in Depth including deterrence, intrusion and tamper detection, physical delay, access control, surveillance, and response capabilities (Fennelly 2003; Garcia 2008; Williams 1981). Therefore, treatment draws on a security professional's operational and technical (engineering) body of knowledge. These are applied to system variables as either human practices or individual situational controls, or environmental design measures or interrelated subsystems, combined as a complex physical security system.

In this context, treatment aims to commission the structural or operational components ensuring compliance with the regulatory framework, codes of practice, and other technical specifications to meet the operational objectives set in the inference phase. Such an approach also recognizes the hierarchical structure of complex engineering systems, in which subsystems are themselves comprised of components that are interrelated. At the treatment level, a physical security system constitutes an engineering solution interrelated accordant with scientific principles of analysis and synthesis to understand component and system efficacy.

Best practice applies components and subsystems that achieve the functions of physical security through their ability to collectively deter, or sequentially detect, delay, and respond against unauthorized actions. Treatment elements are evaluated using relevant codes, standards, and defined performance metrics. The use of and compliance with Codes and Standards is well supported in the security literature (See Atlas 1981; Craighead 2003). For example, Atlas (1981, p. 89) highlighted that codes are written as either performance or design specifications,

identifying performance as statements of contextual achievement, for instance, delaying a defined attack type for a defined period, whereas design specifications establish building construction requirements, referencing particular material selection and methods of construction.

Therefore, best practices method in physical security treatment epitomizes the engineering design process, which includes project realization through system definition and modelling, environmental design, product design and selection, component evaluation, installation, integration, and commissioning based on established criteria. Collectively, these processes functionally achieve the security strategy, which must comply with the operational regulatory environment.

Intrusion Detection

The technical subsystem of detection is the Intrusion Detection System (IDS), designed and commissioned accordant with established security zones (see ▶ "Intrusion Detection Systems" entry in this encyclopedia). The IDS is supported by other subsystems, such as active and passive electronic surveillance technologies for assessment and awareness purposes, lighting infrastructure and other security technologies. Also captured within the technological design component is the electronic communications system, which facilitates the linking of human operators and technical componentry. The performance measures for this subsystem draw on various codes and standards within a jurisdictional context, and probability theory calculated as the likelihood of threat detection.

Movement Control

Another technical subsystem of control is the Access Control System (ACS). ACS is used for controlling movement of people and objects, including portal entry and egress, credentials and barriers, and other delay components. Theoretical underpinnings include principles such as credentials that provide something you have (encoded key or card), know (identification code), or are (biometrics) (Smith and Brooks 2013, pp. 159–171).

Response

The situational crime prevention measure or integrated engineered physical protection system are commissioned to facilitate an effective response against a defined threat. Garcia (2008) states this may include immediate on-site response or after the event recovery. Nevertheless, response relates to the performance measures set following diagnosis. The evaluation of on-site response is based on defined performance measures including the denial level and corresponding probability of interrupting and, where necessary, neutralizing the defined threat. Jurisdictional legal frameworks will guide the setting of response standards and therefore, best practice; however, all response behaviors lie on a continuum. Response must be legal and as a minimum considered against a reasonably foreseeable defined threat but may also include extraordinary events.

Modelling Physical Security Best Practice Treatment

Best practices in physical security treatment involve systems modelling, which seeks to develop a simplified, idealized representation that mimics the behavior of the real system to an acceptable level of accuracy (Dandy et al. 2018). Modelling may occur for individual treatment measures or for a large-scale physical protection system, with a focus on evaluation of effectiveness against a defined threat.

Garcia's (2008) publication of the Estimate of Adversary Sequence Interruption (EASI) model for physical security system evaluation highlighted this view into the idea of best practices for physical security. EASI represents a deterministic system, aiming to achieve the same outcome consistently and drawing on probability theory. Such mathematical modelling studies the behavior of existing systems or proposed systems to identify a system state and possible improvements (Dandy et al. 2018).

Physical Security System Management

The physical security strategy is commissioned compliant with performance or technical

specifications in a manner that meets operational objectives; nevertheless, it must be managed and maintained as a system. Therefore, best practices would have physical security managed as a system, based on the efficacy of its objectives being to deter, detect, delay, and respond against defined threats. Consequently, once individual security elements have been systematically commissioned, the measurable processes that ensure efficacy need to be maintained at their commissioning levels. As such, best practice in physical security must also include system decay theory (Coole 2010).

Conclusion

Best practices in physical security draw on its body of knowledge (academic basis) to *diagnose* the security problem, *infer* to set the protection strategy and operational objectives, and *treat* to achieve optimal mitigation with physical components that comply with relevant codes, standards, and guidelines. Diagnosis commences with a threat assessment of adversary groups or individuals, their intent, and capability. Then, a vulnerability assessment ensures that the system is threat driven, supported by risk assessment to understand the significance of the threat within the defined context.

Inference sets the physical security strategy, which demarcates and divides space into *security zones* of protection, sets the level of protection across these zones based on risk (consequences), and establishes system performance measures. Such a security strategy is realized through treatment, where the engineering design process defines the operational standards, facilitates the design and selection of components, their installation and integration, and ultimately their commissioning. However, consistent with decay theory, the system must be managed as an open system, where decay is identified and counted to maintain the security systems commissioned state or updated accordant with the changing threat environment. The benefits for professionals in undertaking their occupational work accordant with best practice is that they will mitigate the threats which pose a risk to the best of their ability within the corpus of knowledge available at that time; therefore, meeting reasonable care requirements under their professional duty obligations.

Cross-References

- ▶ Criminals: Motives
- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats
- ▶ Insider Threat
- ▶ Intrusion Detection Systems
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Exterior Application
- ▶ Physical Security: Interior Applications
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Risk Analysis: National and International Standards
- ▶ Security Management
- ▶ Security: Theories

References

Abbott. (1988). *The system of professions: An essay on the division of expert labor*. Chicago: The University of Chicago Press.

American Institute of Architects. (2003). *Security planning and design: A guide for architects and building design professionals*. Hoboken: Wiley.

ASIS International. (2015). *Physical security principles*. Alexandria: ASIS International.

Atlas, R. I. (1981). Crime prevention through building codes. In J. Stroik (Ed.), *Building security ASTM STP 729* (pp. 88–97). Baltimore: American Society for Testing and Materials.

Bertalanffy, L. V. (1950). An outline of general systems theory. *The British Society for the Philosophy of Science, 1*(2), 134–165.

Clarke, R. V. G. (1980). Situational crime prevention: Theory and practice. *The British Journal of Criminology, 20*(2), 136–147.

Coole, M. P. (2010). *Theory of entropic security decay: The gradual degradation in effectiveness of commissioned security systems*. Masters of Science, Edith Cowan University.

Coole, M., Brooks, D. J., & Minnaar, A. (2018). Educating the physical security professional: Developing a science-based curriculum. *Security Journal, 31*(2), 524–547.

Craighead, G. (2003). *High-rise security and fire life safety* (2nd ed.). Woburn: Butterworth-Heinemann.

Dandy, G., Daniell, T., Foley, B., & Warner, R. (2018). *Planning and design of engineering systems* (3rd ed.). Boca Raton: CRC Press.
Fennelly, L. J. (2003). *Effective physical security* (4th ed.). Waltham: Butterworth-Heinemann.
Fennelly, L. J., & Crowe, T. (2013). *Crime prevention through environmental design* (3rd ed.). Oxford: Elsevier Science & Technology.
Fischer, R. J., Halibozek, E., & Green, G. (2008). *Introduction to security* (8th ed.). Burlington: Butterworth-Heinemann.
Garcia, M. L. (2008). *The design and evaluation of physical protection systems*. Boston: Butterworth-Heinemann.
Higgins, C. E. (1989). *Utility security operations management: For gas, water, electric and nuclear utilities*. Illinois: Charles C Thomas Publisher.
ISO. (2018). *ISO 31000 risk management – guidelines*. Geneva: International Organization for Standardization.
Jacobs, J. (1961). *The death and life of great American cities*. New York: Modern Library.
Lab, S. P. (2014). *Crime prevention: Approaches, practices and evaluations* (8th ed.). Waltham: Elsevier.
Newman, O. (1972). *Defensible space: People and design in the violent city*. London: Architectual Press.
Parker, M. (Ed.). (2007). *Dynamic security: The democratic therapeutic community in prison*. London: Jessica Kingsley.
Sennewald, C. A. (2013). *Security consulting* (4th ed.). Waltham: Butterworth-Heinemann.
Smith, C. L. (2003). *Understanding concepts in the defence in depth strategy*. School of Engineering and Mathematics. Edith Cowan University, Perth.
Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*. Burlington: Butterworth-Heinemann.
Standards Australia. (2006). *AS/NZS HB167, security risk management*. Canberra: Standards Australia.
Talbot, J., & Jakeman, M. (2009). *Guide to SRMBOK physical security specifications and postures*. Canberra: Jakeman Business Solutions.
The American Institute of Architects. (2004). Security Planning and Design: A guide for architects and building design professionals. Hoboken, NJ: John Wiley & Sons.
Underwood, G. (1984). *The security of buildings*. London: Butterworths.
Williams, J. D. (1981). Design considerations for high-security interior intrusion detection systems. In J. Stroik (Ed.), *Building security ASTM STP 729* (pp. 140–176). Baltimore: American Society for Testing and Materials.
Wyss, G. D. (2009). Quantifying the degree of balance in physical protection systems. Presented at the INMM 50th annual conference, Tucson, AZ: U.S. Deptartment of Energy.
Zipser, B. (1999). Professionals and the standard of care. *Torts Law Journal, 7*(2), 167.

Further Reading

ASIS International. (2009). *Facilities physical security measures guideline*. Alexandria: ASIS International.
Attorney-General's Department. (2015). *Physical security management guidelines: Security zones and risk mitigation control measures*. Barton: Australian Government.
O'Shea, L. S., & Awwad-Rafferty, R. (2009). *Design and security in the built environment*. New York: Fairchild Books.

Physical Security: Exterior Application

Rae Zimmerman[1] and Carlos E. Restrepo[2]
[1]Institute for Civil Infrastructure Systems, Robert F. Wagner Graduate School of Public Service, New York University, New York, NY, USA
[2]Tandon School of Engineering, New York University, New York, NY, USA

Keywords
Physical security · Vehicle ramming · Infrastructure protection · Social vulnerability · Safety · Terrorism · Intentional acts of violence · Natural hazards

Definition

Exterior application of physical security entails a system that "integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks" (Garcia 2008, p. 1).

Introduction

Attention has been drawn to the use of physical security to reduce risks of exposure and consequences of intentional attacks on exteriors. Such measures also can be applied to unintentional weather-related and other natural hazards and accidents. Garcia (2008, p. 2) distinguishes the term security from safety. The term security is restricted to the outcome of "an attack by a

malevolent human adversary," and safety is applied to "the operation of systems in abnormal environments" (Garcia 2008, p. 2). Karlos et al. (2017, p. 3) provide a similar distinction. Dictionaries broaden the definition of security. For example, the Oxford Dictionary (2019) defines security as "The state of being free from danger or threat." The definition implies that physical security can go beyond the more restrictive definition of intentional acts, and though these broader types of threats are beyond the scope of this entry, they are discussed briefly for comparative purposes and for mutual reinforcement.

The concept of physical security in this entry initially addresses prevention of intentional intrusions and is extended briefly to natural hazards given the wide range of attacks society faces from both sources and the fact that many malevolent acts can result in outcomes like those occurring from natural hazards. For example, Garcia (2008) cites fires resulting from terrorist attacks as an example of the overlap. Another example includes floods that result from attacking dams on waterways (see ▶ "Critical Infrastructure: Water and Wastewater Systems Sector" in this encyclopedia). The opposite can also occur. For example, natural hazards can create conditions that lead to malevolent acts of vandalism, where looting has occurred following such events.

Physical security systems are defined by Garcia as physical protection systems (2008, p. 1): a system that "integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks." The purposes of physical security, regardless of whether the risks, threats, or hazards are natural or human in origin, are those suggested by Garcia for malevolent human actions (Garcia (2008, pp. 2–7): to prevent, deter, delay, divert, or detect movement and reduce damage.

Attacks from intentional and unintentional human actions are of critical concern given what appears to be a growing security problem in terms of the frequency, number of lives affected, and economic impacts of both types of acts. This entry focuses on physical security mechanisms primarily used to address intentional violent human acts that typically involve infrastructure systems. Given the widespread use of infrastructure systems, attacks on them have the potential for significant human exposure. Weaponized vehicles or "vehicle-ramming" incidents that use transportation infrastructure are emphasized here. Klein and Independent Democratic Conference (2017, p. 3) using the Global Terrorism Database cite an increase internationally in fatalities from 10 to125 and injuries from 53 to 523 over the period 2006 to 2016 from "terrorist vehicle-ramming attacks" (see ▶ "Terrorism: International" in this encyclopedia).

Some analogies are also briefly presented for physical protection from natural hazards to compare with intentional malevolent acts and to explore the possibility of synergies for protective measures between them. Cyberattacks against infrastructure are also covered briefly given the increasing incidents in that area especially with respect to new technologies such as autonomous vehicles (see ▶ "Critical Infrastructure: Transportation Systems" in this encyclopedia). Although there are many forms and locations of intrusion, the focus in this entry is on external systems rather than internal or building-related systems though the two may be related.

Attacks that have prompted physical security take many forms that often have different origins and purposes, and security is used to at least reduce the consequences of such acts. The importance of security as a public priority is indirectly reflected in the typically high rank of terrorism among the priorities measured by the Pew Research Center (2019) through surveys, at least for the period 2011–2018 (p. 8; see ▶ "Terrorism: Domestic" in this encyclopedia).

First, the concept of physical security has been introduced and defined in the first section above. Second, examples of the technologies being used, criteria for selection, and selected illustrative costs are provided for different types of security measures. Third, actions that have prompted the use of physical security are discussed, focusing on vehicle ramming. Finally, new directions are introduced including broader economic impacts to diversify physical security measures to support multiple social purposes and to promote soft versus hard physical protections.

Types of Physical Security Systems, Selection Criteria, and Selected Costs

Physical security facilities and systems are generally divided into those that are passive or active (Garcia 2008). Passive barriers are also called inactive, and active ones have been referred to as retractable/moving either manually or automatically (Oakes 2016). There are many support systems accompanying these facilities such as information technologies and electric power that may also warrant security measures (see ▶ "Human-Made Disasters: Electric Power and Transit Linked Outages" in this encyclopedia). Many forms of physical security are used depending on where and what kind of protection is needed. Barriers for transportation systems include, for example, barriers, bollards, and gates. Tables 1 and 2 contain a list of some different types. Extensive reviews of types of physical security facilities exist (Oakes 2016; Hathaway and Hammar 1989; U.S. Department of Homeland Security (DHS) 2010, 2013; U.S. Department of Veterans Affairs 2007).

Selection Criteria

Criteria for barrier selection for physical security depend on the objectives, and these generally include availability, constructability, performance in terms of the ability to withstand impacts, cost, and aesthetics (U.S. Department of Homeland Security 2014). Cost has been a particularly important selection criterion.

Selected Costs

Tables 1 and 2 contain a summary of illustrative costs for passive and active barriers from Oakes (2016), the US Department of Defense (DOD) (1999), and the US Department of Veteran Affairs (DVA) (2007). These sources also provide an extensive list of costs often subdivided by individual components and support facilities by their characteristics. The US DHS (2014, p. 53) provides examples for a "single active vehicle barrier" ranging from $10,000 to $65,000. The US EPA (2004) has also produced cost estimated for security products, primarily for water supply.

Actions Leading to Physical Security

The cases of intentional human actions addressed here are general, unwanted, and often illegal intrusion onto properties usually with the intent to disrupt. Although some are less destructive than

Physical Security: Exterior Application, Table 1 Costs of selected passive barriers (illustrative)

Type of passive barrier	US DOD	US DVA	Oakes
Jersey barrier	$40/ft	$435–915	
Fixed bollard	$600		$2,600–2,800
Fixed bollard: concrete	$520		
Removable bollard			$3,500
Security planter	$80/ft	$690–1,950	

Sources: U.S. Department of Defense (DOD) (1999), pp. 91–92; U.S. Department of Veteran Affairs (DVA) (2007), pp. 3–5; Oakes (2016), pp. 3–4. Oakes data is for equipment costs.
Note: Costs are highly variable, often a function of size and materials. Most of the estimates are for equipment costs only, where the distinction is made.

Physical Security: Exterior Application, Table 2 Costs of selected active barriers (illustrative)

Type of active barrier	US DOD	US DVA	Oakes
General	$9–40,000		
Wedge crash barriers		$71,500–78,500	
Crash barriers		$72,500–101,500	
Raised bollard crash barriers		$24,200–34,400	
Retractable bollards: hydraulic			$40–48,000

Sources: U.S. Department of Defense (DOD) (1999), pp. 91–92; U.S. Department of Veteran Affairs (DVA) (2007), pp. 3–5; Oakes (2016). pp. 3–4. Oakes data is for equipment costs.
Note: Costs are highly variable, often a function of size and materials. Most of the estimates are for equipment costs only, where the distinction is made.

others, they reflect intrusive means that could potentially lead to more destructive acts. The Oklahoma City bombing of the Alfred P. Murrah Federal Building (April 19, 1995) was a key event – a turning point – signaling the need for physical security. The emphasis in this section is on a type of action that has been given a great deal of attention – vehicle ramming. Other intrusions are also discussed briefly, namely, scaling of bridges and cyberattacks, primarily on infrastructure, and their physical security implications.

Vehicle Ramming

Over the course of many decades but most recently since the World Trade Center attacks, vehicles have been weaponized for the purpose of destroying life and property. This is an international phenomenon. Karlos et al. (2017, p. 3) define vehicle ramming as "the use of vehicles (cars, vans, trucks etc.) . . . as a weapon against human targets by terrorists and other type of extremists in their effort to maximize casualties, gain global attention and inflict fear to the population." Karlos et al. (2017, p. 2) estimate that from 2011 to 2017, the number of attacks and the death toll from vehicle ramming have generally increased. They indicate that perpetrators range from single individuals to terrorist organizations and occur at multiple locations with the common denominator being places where relatively large numbers of people congregate (Karlos et al. 2017, p. 2). The potential exists for autonomous vehicles to be used for such purposes, though no cases have emerged.

A number of cases around the world show that vehicles can be used to enter busy sidewalks, cycleways, or public spaces used by pedestrians with the intent of running over pedestrians and cyclists and causing death and injury (Jenkins and Butterworth 2017; Erickson and Stanley-Becker 2017; Ward 2017; Lazo 2017; American Bus Association 2017; Windrem and Arkin 2017).

High-profile cases have been reported in the media in the last few years. Table 3 summarizes

Physical Security: Exterior Application, Table 3 Vehicle ramming examples

Date	City/ country	Description	Injuries	Fatalities
July 14, 2016	Nice, France	A truck was used to attack pedestrians on a beach promenade[1]	200	>80
November 28, 2016	Columbus, Ohio, USA	A car was used to attack pedestrians and the driver then used a knife to continue the attack[2]	11	1
December 19, 2016	Berlin, Germany	A tractor trailer was used to attack pedestrians at a market[3]	48	12
March 22, 2017	London, UK	A vehicle was used to attack people on a bridge and the driver then proceeded to attack security guards with a knife[4]	~40	4
August 17, 2017	Barcelona, Spain	A van was used to attack people on a busy thoroughfare[5]	~80	~13
October 31, 2017	New York City, USA	A truck was used to attack pedestrians and bicycle riders in a walkway/bikeway in Lower Manhattan[6]	~12	8
April 7, 2018	Münster, Germany	A van was used to attack people outside a restaurant[7]	~20	3
April 23, 2018	Toronto, Canada	A van was used to attack pedestrians on a busy street[8]	15	10

References:
[1]Vinograd and Ing 2016
[2]Shapiro et al. 2016
[3]Simon et al. 2016
[4]Bennhold and Castle 2017
[5]Bolon et al. 2017
[6]Almukhtar et al. 2017
[7]Danner 2018
[8]BBC News 2018

some of these attacks and selected impacts. In reaction to such incidents, physical security systems acting as barriers in a variety of forms have been used for prevention. As the size of vehicles used in such attacks increased, other mechanisms have been invoked such as the placement of large trucks, e.g., sanitation trucks filled with sand placed nose to nose to block streets. The use of weaponized vehicles to cause harm in cities around the world has led to the deployment of bollards and security barriers that can prevent vehicles from entering areas that are used by pedestrians and bicycle riders (Quito 2016; Bliss 2017).

Figures 1 and 2 show the kinds of barriers that have been implemented in Lower Manhattan near the scene of the 2017 vehicle attack (Almukhtar et al. 2017). These barriers prevent unauthorized vehicles from entering Hudson River Park, which has a high number of pedestrians and bicycle riders.

Scaling Bridges

Bridge access primarily along cables has become a form of intrusion that is disruptive and dangerous, though generally not resulting in loss of life. Other structures have been scaled as well. Examples of the scaling of bridges in 2014 are given below, a year when several of these events occurred:

- July 22, 2014. Two German tourists/artists scaled the Brooklyn Bridge and replaced the American Flag with a white flag (McKinley 2014).
- August 24, 2014. A Russian tourist scaled the Brooklyn Bridge during the day (McKinley 2014). The response to these incidents on September 2, 2014, was the placement of metal screens on bridge cables as a barrier to intrusions (Morales and Shallwani 2014).
- November 16, 2014. A French tourist scaled the Brooklyn Bridge, climbing over a barrier (Pervaiz 2014).

Physical Security: Exterior Application, Fig. 1 Physical barriers on Hudson River Park near Houston Street, New York City. (Source: Photo provided by Carlos E. Restrepo)

Physical Security: Exterior Application, Fig. 2 Physical barriers on Hudson River Park near Chambers Street, New York City. (Source: Photo provided by Carlos E. Restrepo)

One type of barrier that is used on bridges to prevent scaling incidents is shown in Fig. 3. These physical security facilities are used in conjunction with screens and other types of barriers such as gates to reinforce barriers to access and have been used on New York area bridges; they are considered especially effective when installed at low points in the cables where they are closer to pedestrian paths (Morales 2014).

Computer-Related Intrusions (Cyberattacks)

Computer controls now dominate many physical systems and present vulnerabilities in the form of cyberattacks and other computer intrusions. These have been reported by ICS-CERT for infrastructure disruptions, and some attacks increased between 2011 and 2015 (Zimmerman 2017). Prior to that, simple laptops off-site were used to disrupt infrastructure operations such as spillage of water and wastewater (U.S. Government Accountability Office 2007, pp. 6–7). As information technologies become more common in the operation and control of infrastructure, including vehicles, vulnerabilities to cyberattacks will have to be managed. Many cyber security systems work together with physical security systems (Zimmerman and Dinning 2017).

Physical Security: Exterior Application, Fig. 3 Bridge cable barrier to prevent intrusion. (Source: Photo provided by Rae Zimmerman)

Analogies from Unintentional Breaches of Physical Security

The challenge that physical security poses is reflected in vulnerabilities that have arisen in the context of unintentional attacks with outcomes like those originating from intentional acts. For infrastructure, intruders accessing infrastructure facilities could cause damages similar in magnitude to unintentional acts. Some examples are noteworthy of unintentional disabling of infrastructure systems from computer failures and natural hazards such as lightning strikes and other weather-related hazards that commonly occur that produced outcomes like deliberate intrusions. Examples of computer failures that have affected rail transportation (Zimmerman 2012) are:

1. On August 20, 2003, CSX rail shut down from a computer system failure (InformationWeek 2003).
2. On May 25, 2006, Amtrak and NJ Transit were disrupted from a failed 4-year-old computer part that provided power restoration orders (Associated Press 2007; Wald 2007).
3. On September 29, 2011, major disruptions of the Long Island Railroad occurred from a lightning strike and the associated failure of a new computer system (Metropolitan Transportation Authority 2011).

Another type of incident occurred in 2007 where magnetic structures were catapulted onto bridges and other steel structures in many US cities resulting in massive shutdowns of infrastructure, and some of those cities were put on alert due to fears of intentional terrorist acts (Chung 2007). The originators were advertisers, law enforcement officials had them removed, and the settlement was cited as $2 million, half of which was for the infrastructure disruptions (Zezima 2007). Although these actions were intentional and did not appear to be malevolent or linked to terrorism, they did point to vulnerabilities in access that are relevant to physical security.

Going Forward: Some Solutions

Information technologies are now used with physical security for protection and these two components need to be integrated with one another. On the one hand, information technologies can enhance and strengthen physical barriers, and, on the other hand, physical barriers are often needed to provide physical support for information technology devices (Zimmerman and Dinning 2017). One notable example is CCTV used to detect perpetrators. It was used to identify London train bombers in 2004. The deployment of CCTV is often flexible, for example, it can be mounted on physical rail transit structures (see ▶ "Rail (Train) Security" in this encyclopedia).

Physical security barriers can be coordinated to address multiple threats that have similar outcomes. Protection systems for natural hazards

share some similar purposes in common with security threats. Examples of technologies used for natural hazards involved in flooding are designed to seal off areas from water impingement. Examples range from sandbags, "Hesco" baskets, and "Tiger Dams" at relatively smaller scales to massive flood walls and massive instream barriers such as the Thames Barrier. These structures also at least reduce or complicate access by malevolent actors. In the aftermath of Superstorm Sandy, for example, a project in Red Hook, Brooklyn, is contemplating using barriers that are designed to serve multiple purposes. These barriers can help reduce flooding, create green space, and house battery storage capacity that can provide electricity when there is a blackout (Rosenberg 2017). These barriers could also be designed to support backup services for other critical infrastructure systems such as telecommunications. This type of barrier design suggests that such structures can serve multiple goals and can contribute to improving safety and security during extreme weather events.

The implementation of barriers has costs and benefits. These can be difficult to quantify. The most obvious benefit is that they can prevent something like a vehicle attack. However, once barriers are implemented, it is difficult to measure the impacts they may have helped to prevent. Another benefit is that pedestrians and bicycle users may feel more comfortable using sidewalks, parks, and bikeways if they see security measures in place. On the other hand, using barriers in dense urban environments can be a nuisance to pedestrians and bicycle riders trying to navigate busy sidewalks and bikeways. These kinds of barriers can also make it difficult for local authorities to use maintenance, security, and emergency vehicles in areas where they may be needed.

A 2012 study used a large-scale infrastructure construction project to assess whether the use of barriers had significant economic costs in a neighborhood (Zimmerman and Restrepo 2012). The study used large physical barriers and structures deployed during the construction of the Second Avenue Subway in Manhattan to understand potential costs related to housing and business activity. A literature review suggested the barriers and disruptions had a negative impact on rents close to these structures. However, the authors looked at the assessed property values of a random sample of buildings in the area and compared values before and after the beginning of the construction project and found no significant impact on this measure. Extrapolating the kinds of costs associated with large-scale construction projects to physical security barriers has some limitations since the former tend to use much larger barriers and structures.

In response to environmental and social concerns associated with hard physical barriers, softer approaches to protection have emerged. Hard infrastructure has been considered a contributor to increased vulnerabilities for natural hazards (Logan et al. 2018). For natural hazards, green infrastructure has been promoted for many purposes such as absorbing water, pollutants, heat, etc. The concept of water-absorbing structures has been popularized in the Netherlands, among other places throughout the world. Water tunnels that act to channel road traffic during dry weather and water in wet weather have also been introduced, for example, in Kuala Lumpur, Malaysia (Zimmerman 2012, pp. 115, 149; ITS International 2012). Parkland has provided an outlet for combining environmental protection and social goods as an alternative to physical structures (Beitsch 2019).

Similarly, for physical security, traditional hard barriers have been designed for aesthetic and recreational purposes. Physical barriers can be used in combination with other measures to improve security. These include landscaping to create green buffers between streets and sidewalks and creating auto-free areas in parts of cities with high numbers of pedestrians (Ventiere 2017; Garfield 2017). In addition, information about traditional vehicle collisions with pedestrians can help transportation and security planners identify areas where pedestrians may be at risk and where physical barriers can reduce harm.

Conclusions

Physical security is a very real need given the numerous incidents that have occurred, many with severe social consequences not only as direct

loss of life and injury but also the often difficult to estimate psychological toll. Physical security is often an initial response to intentional acts as it is with other kinds of threats posed by natural hazards. Ways in which protection for multiple hazards can be provided are important considerations given the very large investment often required to support such security measures. Also, a very important direction is to promote ways to provide socially beneficial uses of such barriers, for example, for aesthetics and recreation.

Cross-References

- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector
- ▶ Emergency Management: Crisis Management and Response
- ▶ Human-made Disasters: Electric Power and Transit Linked Outages
- ▶ Rail (Train) Security
- ▶ Terrorism: Domestic
- ▶ Terrorism: International

Acknowledgments This work was supported by the following grants:

"Dynamic Resiliency Modeling and Planning for Interdependent Critical Infrastructures," funded by the Critical Infrastructure Resilience Institute (CIRI), U. of Illinois, Urbana-Champaign, supported by the US Department of Homeland Security under Grant Award #2015-ST-061-CIRC01

The National Science Foundation under Cooperative Agreement #1444755, the Urban Resilience to Extremes Sustainability Research Network (UREXSRN)

"Critical Resilient Interdependent Infrastructure Systems and Processes (CRISP) Type 1: "Reductionist and integrative approaches to improve the resiliency of multi-scale interdependent critical infrastructure," funded by the NSF (#1541164)

"Developing Secure Strategies for Vehicular Ad hoc Networks in Connected and Autonomous Vehicles," from C2SMART, NYU Tandon School of Engineering, US Department of Transportation. US DOT award number 69A3551747124

Disclaimer: Any opinions, findings, views, conclusions, or recommendations expressed in this material are those of the authors and not to be interpreted as necessarily representing the official policies, either expressed or implied, of the National Science Foundation, the US Department of Homeland Security, or the US Department of Transportation.

References

Almukhtar, W., Griggs, T., Lee, J.C., Fessenden, F., Rebecca Lai, K.K., Patel, J., Saget, B., & Singhvi, A. (2017, October 31). Trail of terror in the Manhattan truck attack. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2017/10/31/nyregion/manhattan-truck-attack.html

American Bus Association. (2017). ABA member alert: Vehicle ramming. Retrieved from https://www.buses.org/news/article/aba-member-alert-vehicle-ramming

Associated Press. (2007, February 24). Amtrak blames outage on computer flaw. *Associated Press* online.

Beitsch, R. (2019, February). U.S. cities trade seawalls for parks. *Planning, 85*, 10–11.

BBC News. (2018, April 24). Toronto van: Ten dead and 15 injured as pedestrians are hit. Retrieved from https://www.bbc.com/news/world-us-canada-43873804

Bennhold, K., & Castle, S. (2017, March 22). Deadly attack near U.K. Parliament; Car plows victims on Westminster Bridge, *The New York Times*. Retrieved from https://www.nytimes.com/2017/03/22/world/europe/uk-westminster-parliament-shooting.html

Bliss, L. (2017, November 1). Vehicle attacks are not inevitable. *CityLab*. Retrieved from https://www.citylab.com/transportation/2017/11/vehicle-attacks-are-not-inevitable/544598/

Bolon, A-S., Karasz, P., & McKinley, J. C., Jr. (2017, August 17). Van hits pedestrians in deadly Barcelona terror attack. *The New York Times*. Retrieved from https://www.nytimes.com/2017/08/17/world/europe/barcelona-catalunya-van.html

Chung, J. (2007, February 1). Aqua Teen Hunger Force mooninites don't scare NYC. *Gothamist*. Retrieved from https://gothamist.com/2007/02/01/aqua_teen_hunge.php

Danner, C. (2018, April 7). 3 dead after van drives into crowd in Münster, Germany. *New York Magazine*. Retrieved from http://nymag.com/intelligencer/2018/04/3-killed-after-van-drives-into-crowd-in-munster-germany.html

Erickson, A., & Stanley-Becker, I. (2017, March 22). How ramming cars into crowds became a major terror tactic. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2017/03/22/as-the-london-attacks-show-the-sedate-sedan-can-be-turned-into-a-deadly-unpredictable-weapon/

Garcia, M. L. (2008). *Design and evaluation of physical security systems* (2nd ed.). Amsterdam: Elsevier Butterworth-Heinemann.

Garfield, L. (2017, August 16). 10 cities that are starting to go car-free. *Business Insider*. Retrieved from http://www.businessinsider.com/cities-going-car-free-2016-8/#oslo-norway-will-implement-its-car-ban-by-2019-1

Hathaway, W. T., & Hammar, P.K. (1989). Perimeter barrier selection guide. U.S. Department of State and U.S. DOT. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a233839.pdf

InformationWeek. (2003, August 20). Computer virus brings down train signals. Retrieved from http://www.

informationweek.com/computer-virus-brings-down-train-signals/d/d-id/1020446?

ITS International. (2012). Success of Kuala Lumpur's dual purpose tunnel. Retrieved from https://www.itsinternational.com/categories/detection-monitoring-machine-vision/features/success-of-kuala-lumpurs-dual-purpose-tunnel/

Jenkins, B. M., & Butterworth, B. R. (2017). Terrorist vehicle attacks on public surface transportation targets. Mineta Transportation Institute. Retrieved from http://transweb.sjsu.edu/sites/default/files/terrorist-vehicle-attacks-on-public-surface-transportation-targets_0.pdf

Karlos, V., Larcher M., & Solomos G. (2017). *Review on vehicle barrier protection guidance*. Luxembourg: European Union. Retrieved from http://publications.jrc.ec.europa.eu/repository/bitstream/JRC109289/kjna28938enn.pdf

Klein, J. D. S., & Independent Democratic Conference. (2017, November). *Vehicle ramming prevention*. Albany: The New York State Senate. Retrieved from https://www.nysenate.gov/sites/default/files/press-release/attachment/vehicle_ramming_prevention_full_report.pdf

Lazo, L. (2017, July 9). Vehicles as weapons of terror: U.S. cities on alert as attacks hit the West. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/trafficandcommuting/vehicles-as-weapons-of-terror-us-cities-on-alert-and-preparing-as-attacks-are-on-the-rise-in-the-west/2017/07/09/806be4be-55eb-11e7-ba90-f5875b7d1876_story.html

Logan, T. M., Guikema, S. D., & Bricker, J. D. (2018, September). Hard-adaptive measures can increase vulnerability to storm surge and tsunami hazards over time. *Nature Sustainability, 1,* 526–530.

McKinley, J. C., Jr. (2014, August 25). Tourist is held after climb on Brooklyn Bridge cable. *New York Times*. Retrieved from http://www.nytimes.com/2014/08/26/nyregion/tourist-is-held-after-climb-on-brooklyn-bridge-cable.html

Metropolitan Transportation Authority (MTA). (2011, October 24). Preliminary review September 29, 2011 lightning strike at Jamaica. Retrieved from http://web.mta.info/supplemental/lirr/images/09-29-2011_LightningStormPR.pdf

Morales, M. (2014, October 5). Brooklyn Bridge gets more barriers, *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/brooklyn-bridge-gets-more-barriers-1412564568

Morales, M., & Shallwani, P. (2014, September 2). New barriers added to Brooklyn Bridge to block intruders. Metal screens may thwart unauthorized climbers after recent stunts. *Wall Street Journal*. Retrieved from http://online.wsj.com/articles/new-barriers-added-to-brooklyn-bridge-to-block-intruders-1409706761

Oakes, C. G. (2016). *Bollard: Crash-and attack-resistant models, whole building design guide*. Washington, DC: National Institute of Building Sciences. Retrieved from https://www.wbdg.org/resources/bollard-crash-and-attack-resistant-models

Oxford University Press. (2019). The Oxford dictionary. Security. Retrieved from https://en.oxforddictionaries.com/definition/security

Pervaiz, S. (2014, November 17). French tourist charged after climbing on Brooklyn Bridge. *Wall Street Journal*. Retrieved from http://blogs.wsj.com/metropolis/2014/11/17/french-tourist-charged-after-climbing-on-brooklyn-bridge/

Pew Research Center. (2019, January). *Public's 2019 priorities: Economy, health care, education and security all near top of list*. Washington, DC: Pew Research Center.

Quito, A. (2016, July 17). The secret of anti-terror architecture: Your city is probably safer than you realize. *Quartz*. Retrieved from https://qz.com/733374/counter-terrorism-architecture-how-cities-prevent-attacks-without-looking-like-theyre-trying/

Rosenberg, Z. 2017. New looks at KPF's resilient Red Hook utility pods. *Curbed*. Retrieved from https://ny.curbed.com/2017/3/24/15051138/red-hook-utility-pods-kpf-renderings-nyc

Shapiro, E., Katersky, A., Margolin, J., & Levine, M. (2016, November 28). Ohio State University student dead after driving into crowd, stabbing people at OSU campus. *ABC News*. Retrieved from http://abcnews.go.com/US/ohio-state-university-student-dead-driving-crowd-stabbing/story?id=43821371

Simon, D., Ellis, R., & Pleitgen, F. (2016, December 19). Berlin Christmas market: 12 dead, 48 hospitalized in truck crash. *CNN*. Retrieved from http://www.cnn.com/2016/12/19/europe/berlin-christmas-market-truck/index.html

U.S. Department of Defense (DOD). (1999). *Handbook MIL-HDBK-1013/14, selection and application of vehicle*. NFESC: Barriers.

U.S. Department of Homeland Security (DHS). (2010). Dams sector active and passive vehicle barriers guide. Retrieved from https://www.dhs.gov/sites/default/files/publications/dams-vehicle-barriers-guide-508.pdf

U.S. Department of Veteran Affairs (DVA). (2007). Physical security design manual for VA facilities. Cost estimates for physical security enhancements. Retrieved from https://www.wbdg.org/FFC/VA/VAPHYS/va_security_costs_dm_2007.pdf

U.S. DHS. (2014). Guide to active vehicle barrier (AVB) specification and selection resources. Retrieved from https://www.dhs.gov/sites/default/files/publications/Guide-to-Active-Vehicle-Barrier-2014-508.pdf

U.S. DHS (FEMA). (2013). FEMA 430 chapter 4 perimeter security design. Retrieved from https://www.fema.gov/media-library-data/20130726-1624-20490-0371/430_ch4.pdf

U.S. Environmental Protection Agency (EPA). (2004). Security product guide. Active security barriers. Retrieved from https://nepis.epa.gov/Exe/ZyPDF.cgi/940016CG.PDF?Dockey=940016CG.PDF

U.S. Government Accountability Office. (2007, September). Critical infrastructure protection. Multiple efforts to secure control systems are under way, but challenges

remain. GAO 07 1036. Retrieved from https://www.gao.gov/assets/120/118145.pdf
Ventiere, M. (2017, August 14). Soft targets: Stemming the tide of vehicle ramming attacks. *SecurityInfoWatch*. Retrieved from http://www.securityinfowatch.com/article/12352685/soft-targets-stemming-the-tide-of-vehicle-ramming-attacks.
Vinograd, C., & Ing, N. (2016, July 17). Nice attack investigation: Two more detained after truck massacre. *NBC News*. Retrieved from https://www.nbcnews.com/storyline/france-truck-attack/nice-attack-investigation-two-more-arrests-after-truck-massacre-n611066
Wald, M. L. (2007, February 23). New gear, not old, caused 2006 Amtrak blackout. *New York Times*. Retrieved from http://www.nytimes.com/2007/02/23/us/24amtrakcnd.html
Ward, A. (2017, October 31). The New York attack shows why trucks are now the terrorist weapon of choice. *The Vox*. Retrieved from https://www.vox.com/2017/10/31/16587868/new-york-city-attack-truck-october-31
Windrem, R., & Arkin, W. M. (2017, May 4). TSA report warns against truck ramming attacks by terrorists. *NBC News*. Retrieved from https://www.nbcnews.com/news/us-news/tsa-report-warns-against-truck-ramming-attacks-terrorists-n754576.
Zezima, K. (2007, February 6). Turner broadcasting and ad agency to pay $2 million for Boston scare – Americas – International Herald Tribune. *New York Times*. Retrieved from https://www.nytimes.com/2007/02/06/world/americas/06iht-boston.4489496.html?searchResultPosition=37
Zimmerman, R. (2012). *Transport, the environment and security. Making the connection*. Cheltenham/Northampton: Edward Elgar Publishing, Ltd. ISBN 978 1 84980 020 4.
Zimmerman, R. (2017, December). *The cyber and critical infrastructures nexus: Interdependencies, dependencies and their impacts on public services*. White Paper, New York University Center for Cybersecurity. Retrieved from http://cyber.nyu.edu/wp-content/uploads/2017/12/Zimmerman-122717updateEdited-White-Paper-Cyber-and-Critical-Infrastructures.pdf
Zimmerman, R. & Dinning, M. G. (2017). Benefits and needs for an integrated approach to cyber-physical security for transportation. In: *Transportation systems resilience: Preparation, recovery, and adaptation*, E-C226, Transportation Research Board.
Zimmerman, R., & Restrepo, C. E. (2012). *Economics of security*, Unpublished report for the Urban Commerce and Security Study (UCASS) through the Center for Risk and Economic Analysis of Terrorism Events (CREATE). Los Angeles: University of Southern California.

Further Reading

Texas A&M. (2019). Roadside safety and physical security design, testing & performance evaluation. Retrieved from https://groups.tti.tamu.edu/crashtesting/research-areas/

Physical Security: High-Rise Residence and Office Buildings

Seungmug (Zech) Lee
Department of Criminology and Criminal Justice, The University of Texas at Arlington, Arlington, TX, USA

Keywords
High-rise/tall building · Risk assessment · Security · Security for high-rise

Definition

High-rise security refers to a specialized but comprehensive safety and protection approach to prevent, mitigate, minimize, and respond the possible danger and emergency situations to life and property for occupants who reside and/or work in multistory buildings from various natural and human-made threats. Security professionals' predominant areas of responsibilities include lobby concierge, operating and monitoring CCTV, screening visitors and client employees, building inspection, and access control.

Introduction

High-rise buildings provide numerous benefits (e.g., a large amount of living, working space on a small land footprint, and reduction of the costs of providing utilities and services) to residences and offices in urban settings, but such benefits come with security and safety issues and challenges. Since they occupy small and size to erect the structures to reach multiple floors, easily from over 10 stories to near or sometimes over 100 stories, high-rise buildings are by and large tall and closed off all sides with a lot of individuals as either residents or office occupants and diverse activities. Unlike low-rise structures with 1–3 flat buildings, such tall high-rise ones are vulnerable to natural or man-made disasters (e.g., earthquake,

fire, power outage, equipment malfunction, and so on) (see a series of ▶ Human-Made Disasters: Toxic Waste and Residences in this encyclopedia).

To protect the lives and property of the multitudes of people who daily use these facilities, it is essential that high-rise security programs and practices are well planned and executed. Security professionals responsible for the safety and protection of such buildings should ensure that appropriate services and programs are in place to protect residents, office occupants, and the property inside.

This entry will discuss the definition and types of high-rise buildings, security challenges, security issues/threats, security responses, and risk assessment for high-rise buildings.

Types of High-Rise Building

A high-rise building is a tall multistory structure. It can include the following aspects: first, any structure where the height can have a serious impact on evacuation; second, for most purposes, the cutoff point for high-rise buildings is around seven stories; and third, a high-rise structure is considered to be one that extends higher than the maximum reach of available firefighting equipment, which can vary between 75 feet (or 23 meters) and 100 feet (or 30 meters) or about seven to ten stories. The exact height above which a particular building is deemed a high-rise is specified by fire and building codes for the country, region, state, or city where the building is located. Elevators are used as a vertical transportation system, and some utilize escalators to move people between lower floors (Ahrens 2016; Craighead 2009).

Since the late 1800s in the USA, high-rise structure developments have dominated major city skylines for office buildings, hotels, and residentials with the help of safety elevator and steel frames. For example, there were two major eras for erecting the tallest buildings – the early 1930s for the 77-story Chrysler Building and the 102-story Empire State Building and the early 1970s for the 110-story Twin Towers of the NY World Trade Center (WTC) and the 110-story Sears Tower in Chicago. However, since themed-1990s, the new wave of the high-rise building constructions has been on virtually all continents of the globe simultaneously, resulting in ever-denser, ever-taller cities from Moscow to the Middle East, from Shanghai to San Francisco with new security and safety challenges. It is not only the height and geographic spread of tall buildings that have changed but also their types and materials used to construct. Whereas historically the world's tallest buildings have been dominated by office buildings, were built of steel, and were built to project the prowess of an individual corporation, many of the world's new supertalls now contain residential or mixed-use functions, use concrete and composite construction, and have been built to project the vitality of a city on a global scale (Challinger 2008; Craighead 2009).

Most high-rise buildings can be categorized based on their primary purpose – office buildings, hotel buildings, residential buildings, specific-purpose buildings, and mixed-use buildings. An *office building* is a structure designed for the conduct of business, generally divided into individual officers and offering space for rent or lease. In the commercial high-rise buildings, occupants are office workers, visitors, and facility management staff. The term "hotel building" is an all-inclusive designation for facilities that provide comfortable lodging and general food, beverage, entertainment, other "away from home" services, as well as a businesslike environment. There are also hotels that contain residences, known as hotel residences. A *residential building* contains separate residences where a person may live or regularly stay. Each residence has independent cooking and bathroom facilities and may be known as an apartment, a residence, a tenement, or a condominium. Examples of high-rise residential buildings include apartment buildings and student dormitories in urban settings. Occupants are residents, visitors, and building support staff. *High-rise specific-purpose* buildings include hotels, hospitals, educational facilities, retail malls, prisons, and car parks. A *mixed-use building* may contain offices, apartments, residences, and hotel rooms in separate sections of the same building (Ahrens 2008; Challinger 2008; Craighead 2009).

Security Challenges of High-Rise Buildings

There are several reasons why high-rise buildings have become popular among the nations in the world. First, the exploding population in largely urban settings creates an increasing demand for high-rise buildings. Arable land areas are gradually being eaten away by urban spreading through suburban developments. The high-rise building can accommodate many more people on a smaller land than would be the case with low-rise building on the same land. Second, it is generally acknowledged that there has been evident neglect of the human factors in the urban design at the expense of livability and quality of life. The outward expansion of cities into the suburbs has resulted in increased travel time and traffic gridlock. Clustering of buildings in the form of high-rise buildings presents an opportunity for creating open recreation for playgrounds, plazas, parks, and other community areas by freeing up space at the ground level (Craighead 2009).

Some characteristics of high-rise building structures are related to the unique security challenges to security professionals and their operational management, including size, location, anonymity within the building, building contents, occupant characteristics, and physical features (Challinger 2008). For example, due to their *size*, high-rise buildings or very tall buildings can be iconic and targets for security breaches. However, their size may also slow down security response in the case of man-made or natural disaster situations. A good example was the old World Trade Center twin buildings in the Lower Manhattan. It became the first target by 9/11 terrorists. *Anonymity* within the building is an inevitable feature which may make it difficult to tell whether people in a high-rise building should be there or not. They could be legitimate occupants or visitors, and among them a potential offender may not look out of place. Anonymity in a high-rise building may lead to a "not my problem" attitude, making it easier for a criminal to operate unobserved.

Another security challenge is *building contents*. A high-rise building generally provides a concentrated volume of property, making it an attractive target for criminals. Much of that property could be described as CRAVED, an acronym for "concealable, removable, available, valuable, enjoyable, and disposable" (Clarke 1999; Petrossian and Clarke 2014). In commercial buildings, some corporate officers feature expensive fittings and high-value art. Property in upmarket residential buildings also tends to be of high quality. High-rise building *occupants* may not all have the same exposure to or concern about security problems. A tall commercial building may be occupied by low-risk tenants, along with high-risk ones (e.g., controversial or high-profile companies, political organizations, and government offices). High-rise residential buildings may have a mix of owner-occupiers, rental tenants, and public housing residents.

Physical features of a high-rise building provide opportunities for such offenses as elevator crime, stairwell crime, and window crime. Surveys indicate elevator crimes and breakdowns are among the top five concerns of high-rise residents. Most elevator crime seems to comprise personal offenses such as robbery or assault. Stairwells in high-rise buildings are invariably enclosed because of construction codes. They provide another site for robbery and offer escape routes for offenders. Lobbies, corridors, and outside plazas, since they are common areas, often have no specific owner or guardian to help prevent crime and disorder. Windows, if openable, may allow access by cat burglars. People may throw objects from windows, causing criminal damage to any passerby or car parked down the street. In a worst case, a window could be used by a sniper. An example was the Las Vegas mass shooting incident on the night of October 1, 2017. *Locations* are also a security challenge. Many high-rise/tall buildings are located in central business districts in major urban cities. Their proximity to mass transit facilities and ease of access to the general public puts them a particular risk from professional criminals.

Security Issues/Threats

High-rise buildings, just like any other built-in environments, have several security threats.

Some can be observed just like any other built-in settings have; however some are unique to high-rise building atmospheres. Examples of the major security threats surrounding high-rise buildings are crimes, disorder, and building emergencies (Challinger 2008; Craighead 2009; Office of the Fire Marshal 2002; Savage 2005).

Crimes are probably the first security concern for high-rise security professionals. Several criminal behaviors around the high-rise building perimeter are (1) theft and burglary from private spaces, car parks, and delivery docks; (2) property damage, such as graffiti and sabotage, most likely in common areas or car parks; (3) offenses against persons, including general violence, domestic violence, elevator assaults, and confrontations in common areas, such as angry interchanges with doormen or receptionists; and (4) unauthorized access to utilities, including theft of telecommunications or electricity with the possibility of commercial espionage.

Disorder is another security threat for high-rise building security. Disorder behavioral issues include drug dealing from the building, hostage-taking, trespassing, suicide risks, protests, and drunk or drug-affected disorderly conduct in and around the buildings.

Two *building emergencies* become a critical aspect of high-rise building security operations – human-caused and natural disasters. The former includes fire/explosion, bomb threats, biological and chemical threats, suspicious package, infrastructure and elevator failures, electricity blackouts, hazardous materials accidents, and terrorist attacks. The examples of the natural disaster are weather events such as earthquakes, floods, tsunamis, hurricanes, tornados, and snowstorms with heavy snowfall.

Security Responses

Several common security responses for high-rise building structures include diverse security practices, including access control, physical security measures, CCTV (closed circuit television), security officers, security and emergency plans, and occupant involvement (Ahrens 2008; Challinger 2008; Fischer et al. 2019; Savage 2005; see ▶ Physical Security: Video Surveillance, Equipment, and Training in this encyclopedia).

Access control is the primary security practice for a high-rise building. A tall building has the restricted number of entry points from outside, which can direct security team to control better access by people, vehicles, and goods. An access control system combined with alarm capacity and CCTV is the most frequently used security measure in high-rise buildings. The level of access control depends on the major business activities of, the function of, and the volume of both human and vehicular traffic of the building. For example, access to building structures housing sensitive government departments may be highly restricted, whereas general access can be given to visitors at hospitals. High-rise residential buildings may have restricted access control practices. Advanced technology has been integrated into automated access control systems for more effective and efficient practice. Vehicle access in high-rise buildings to parking areas is generally automated, though still some buildings station security officers to check and direct in-and-out vehicular movement. Deliveries to high-rise/tall commercial and residential buildings are controlled and channeled through one access point with a security officer loading dock with CCTV monitoring.

Physical security measures are also used in high-rise buildings as a target hardening method, including locks, reinforced doors and windows, intrusion alarms, lighting, perimeter gates and fences, barricades, and bollards. *CCTV* is widely utilized in high-rise building structures with technological advances. For example, Internet-based CCTV which can be integrated with motion detectors and alarm systems can allow occupants to view movements in tall buildings remotely. *Security officers* are still quite common practice in high-rise office and residential buildings. Uniformed security professionals stationed at the main entrance provide the first line of access control function. They can check all visitors, patrol the perimeters, supervise vehicle traffic and access, monitor CCTV control rooms, and respond to emergencies.

Security and emergency plans are an essential part of security responses in high-rise buildings. In most cases, such plans and procedures are mandated by local security and fire safety regulations with the requirements of fire alarm systems and fire drills with evacuations. Particularly, fire evacuation plans are critical for high-rise buildings where the fire service may not be able to reach higher floors in case of fire with their rescue equipment. *Occupant involvement and awareness* is another critical safety response in high-rise buildings. A security staff needs to communicate effectively with occupants in the buildings for emergency plans by means of mailings, websites, elevator bulletins, email, or meetings. Security training and awareness programs can lead to increased natural surveillance among occupants.

Risk Assessments

Security and life safety needs in high-rise buildings should be determined by identifying specific assets and threats against those assets. An important tool for determining such needs is a risk assessment (Craighead 2009; NIST 2005). *Risk assessment* is the process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls. Risk assessment can utilize security survey and fire prevention survey.

A *security survey* is an exhaustive physical examination of the premises and a thorough inspection of all operational systems and procedures. It may focus on different aspects of a high-rise facility, including the area and businesses in the surrounding neighborhood, the building itself, a particular tenant or resident in the building, or defined aspects of the security operation such as policies and procedures, systems, and equipment. Using a survey checklist of areas to be covered, a security survey should include interior spaces of high-rise buildings, building perimeters, and surroundings. A *fire prevention survey* has similar objectives to a security survey, aiming to ascertain the present fire safety status, to identify deficiencies or excesses, to determine the fire safety protection needed, and to make recommendations to improve the overall safety of high-rise building under evaluation (Craighead 2009, Fischer et al. 2019; see ▶ Fire: Prevention, Protection, and Life Safety in this encyclopedia).

Risk assessments are invaluable in helping high-rise building owners, managers, security and safety directors, and consultants effectively and safely operate tall buildings and thereby reduce premises liability. To identify specific assets and the threats to these assets, assess vulnerabilities or weaknesses to such threats, and devise measures to counter such weaknesses, the security surveys and fire prevention survey are an essential tool. To conduct a thorough analysis of a facility, it is helpful that it be carried out in a methodical fashion.

Conclusion

Since their first appearance during the end of the nineteenth century, the design and construction of high-rise buildings have changed significantly in cities. A boom in high-rise/tall building construction and the use of them impact their security and protection needs, depending on different types of building structure and occupancies. Current security measures include access control, physical security, CCTV, alarm systems, lighting, security officers, emergency plans, and documented procedures. Still, crime, disorder, emergencies, and fear surrounding high-rise buildings are constant issues for security practitioners. There might be no perfect security and safety measures for such high-rise building structures. However, a well-conceived security program will effectively prevent potential security problems, mitigate once an incident occurs, and recover from loss and damages. Such a program should be a comprehensive approach with the aspects of physical security and procedural security and cooperation among occupants.

Cross-References

- ▶ Emergency Management: Evacuations
- ▶ Natural Hazards
- ▶ Physical Security: Video Surveillance, Equipment, and Training.

References

Ahrens, S. (2008). High-rise security from the ground up. *Building Operating Management*, 27–32.

Ahrens, M. (2016). *High-rise building fires*. Quincy, MA: National Fire Protection Association.

Challinger, D. (2008). *From the ground up: Security for tall buildings. An ASIS Foundation Research Council CRISP Report*. Alexandria, VA: ASIS Foundation.

Clarke, R. V. (1999). *Hot products: Understanding, anticipating, and reducing demand for stolen goods* (Police research series, paper 112). London, UK: UK Home Office.

Craighead, G. (2009). *High-rise security and fire life safety* (3rd ed.). Burlington, MA: Butterworth-Heinemann.

Fischer, R. J., Halibozek, E. P., & Walters, D. C. (2019). *Introduction to security* (10th ed.). Cambridge, MA: Butterworth-Heinemann.

National Institute of Standards and Technology. (2005). *Final report on the collapse of the World Trade Center Towers*. Washington, D.C.: U.S. Department of Commerce, National Institute of Standards and Technology.

Office of the Fire Marshal. (2002). *A guide to strengthen emergency management of high-rise and high-risk buildings*. Ontario: Ministry of the Solicitor General.

Petrossian, G. A., & Clarke, R. V. (2014). Explaining and controlling illegal commercial fishing: An application of the CRAVED theft model. *British Journal of Criminology, 54*, 73–90.

Savage, B. (2005). High-rise security remains in the spotlight. *Security Technology and Design*, 62–64.

Further Reading

Atlas, R. I. (2013). *Twenty-first century security and CPTED: Designing for critical infrastructure protection and crime prevention* (2nd ed.). Boca Raton: CRC Press.

Baxter, R., & Lees, L. (2009). The rebirth of high-rise living in London: Towards a sustainable, inclusive, and liveable urban form. In R. Imrie, L. Lees, & M. Raco (Eds.), *Regenerating London: Governance, sustainability, and community in a global city* (pp. 151–172). New York: Routledge.

Kitteringham, G. (2006). *Security and life safety for the commercial high-rise*. Alexandria: ASIS International.

Physical Security: Interior Applications

Alex Alexandrou
John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Physical access control mechanism · Access control system · Credential · Readers · Biometric · Authentication · Control panel · Locks · Wireless solutions · Standards · Security

Definition

Access controls are the mechanisms that monitor, prevent, and control access to essential resources, from buildings and garage doors to network data repositories.

Introduction

As technology becomes increasingly pervasive, access controls are everywhere. Examples of access controls include the use of access cards to gain entry into controlled areas, buildings and parking spaces, the use of biometric authentication to access cell phones, and the use of online credentials to access social media like Facebook and Twitter and credentials required to gain access to work computers.

Access controls are categorized into two types, logical and physical. *Logical access controls* feature connections using hardware, software, identification protocols, authentication, authorization, and accountability (audit), to allow access to a computer system and/or a network resource. *Physical access controls* refer to access to buildings, rooms, and control gates. These controls use key fobs, access cards, mobile device applications (apps), and other tokens to allow access to these areas.

This chapter focuses on *physical access control mechanisms*, specifically their description and functionality, credentials, basic components, system topology and standards, security concerns and risks, system adaptability, and best practices in choosing a system. In conclusion, the chapter describes best practices for maintenance of physical access control systems and suggests that the success of an access control system depends upon its ease of use, communication with and training of users and administrators, integration with other systems, and timely software and security updates.

Main Access Control Components

Keys and locks are the ancestors of modern access control systems. The oldest known lock and key were discovered in the ruins of the palace of Khorsabad near Nineveh (Encyclopedia Britannica n.d.). It dates back to about 4000 B.C. and belongs to the Mesopotamian kingdom of Assyria (de Vries et al. 1993). The lock and key spread to ancient Egypt, then ancient Greece, and ultimately to the Roman Empire.

Today, thanks to the arrival of smart home kits and the Internet of things (IoT), the modest key and lock are becoming obsolete. Computer-based devices that transmit, collect, and share data over the Internet autonomously are quickly replacing them. These include smart home devices like smart locks, which are residential access control systems, smart thermostats, smart light bulbs, and smart security camera systems. A smart lock can replace a front door's key. It can remotely lock and unlock a door, track who enters and leaves, and allow access to visitors. In addition, smart locks and other IoT devices, such as smart security camera systems, can interact with smart home ecosystem and thereby provide a broader home automation.

An enterprise access control system is a more complex and elaborate system that can grant access at multiple entry points and can manage hundreds or thousands of users' access credentials. This kind of system can provide a history of events, a real-time audit trail, and can be integrated with intrusion systems, security surveillance systems, and visitor entry systems.

In an access control environment, an access point may be a door, gate, closet, or an elevator door where the system permits access. A cluster of access points is called a zone. A zone may be used to manage a number of doors in a floor or a building. For example, in a hospital environment, a pediatric floor might have 40 different door types, and all may be managed by a single pediatric zone.

Access Control Software

Access control software is the heart of every meaningful system. It handles a large number of access points, zones, different user levels, calendars, time periods, and time zones. The user interface is handled by web-based software (client-based or web-based applications) that can be accessed from any workstation with the right credentials. Since the application is web-based, the interface between a user and the software may be accessed using the Internet or an intranet through a browser. The access control database or access control list (ACL) resides on a server and is accessed over a network.

Control Panel or Controller

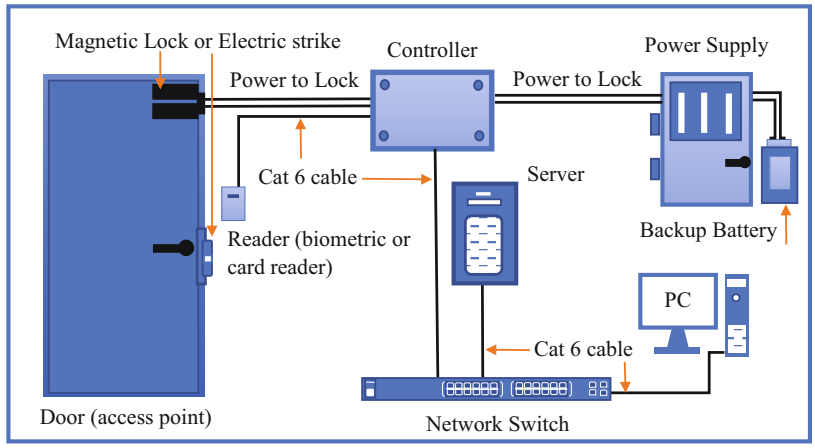
The control panel (controller or control unit) sends the lock a signal to unlock the door when it receives the request from the reader. It then verifies the request with the user's credentials, and if the credentials match, the controller signals to unlock the door (see Fig. 1).

Credentials

The user's credentials in an access control system represent the modern key that allows admission to an entrance. The credentials vary, depending on the user's level of security and level of usage. Credentials may be proximity cards, key fobs, bracelets, mobile apps, passwords, and biometric credentials. In the area of physical security, the most common credential is the RFID card (Bacco et al. 2017).

Locks

The locks (magnetic locks, wireless locks, electric strike, electric mortise door lock, etc.) are the



Physical Security: Interior Applications, Fig. 1 A typical access control setup with the most basic components

essential elements that electrically unlock or lock access points. These different types of locks serve different purposes. Every lock that is not wireless has a wire that supplies power and connects back to the control panel. Wireless locks can be cost-effective and convenient in comparison to wired installations. The disadvantages to wireless lock systems are the cost of their maintenance, for example, updating drivers and replacing batteries. Furthermore, certain locks open spontaneously when electricity is delivered, and certain locks will lock automatically when electricity is suspended. In the event of fire, some locks (front entrance, hospital exit doors, etc.) should open automatically to comply with fire and safety codes and to allow personnel to exit the building during emergencies. A unique lock is the magnetic lock or maglock that uses electromagnetism to control the *locking* apparatus attached to the door and doorframe. This type of lock is used at high traffic and emergency exits that utilize fire safety applications. The appropriate lock to install depends upon the door type and requirements, the location, and the construction material (see Fig. 1).

Readers

Users must employ a reader (biometric, card reader, or keypad) as the first tool to access an entrance. The typical reader scans their credential and sends the request for entry to the controller; it is then sent to the server for authentication. It is the access control database, not the reader that decides whether access is permitted or denied. A combination of readers may be used for additional security (see Fig. 1).

Some readers, especially wireless readers, are built into wireless locks and have their own Internet Protocols (IP). These are used as independent systems and do not communicate with any controller, but instead communicate first with the router and then with the server, which connects via Ethernet or Wi-Fi. Biometric readers utilize mature technologies and are popular with access control systems. Biometric readers identify and authenticate a user based on physical or behavioral characteristics (also known as modalities). Biometric readers can use biometric fingerprint scanners, facial recognition, iris recognition, palm vein recognition scanners, retinal scanners, and voice patterns (Nemeth 2017). However, biometric readers can err by failing to authorize a genuine user. Purchasers should be wary, examining false acceptance rates (FAR), false rejection rates (FRR), accuracy, and anti-spoofing capabilities such as parody and forging.

Exit doors usually employ one reader and a "request to exit" device that allows a person to exit freely, when the user has entered the facility using a credential. The exit device can be a push button or infrared (IR) technology used to request egress by motion detector, which releases the lock. The device communicates with the access control software and instigates free egress. This is an important feature for meeting fire safety code requirements. Access control systems and

more specifically controllers are usually linked to fire alarm systems. In addition, all access points, along with their controllers, readers, request to exit devices, and locks should be equipped with a 4-h backup battery (Norman 2011) and should be connected to a backup generator.

Access Control System Description and Functionality

Description

An access control system allows the end user to manage and screen access to a particular area, entry or exit point in real time. In some cases, for example, in restricting access, companies and agencies are required to adopt access control systems as part of regulatory compliance. Hospitals are required to comply with state, local, and federal requirements like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as with requirements set by independent, not-for-profit organizations like the Joint Commission for Regulatory Compliance. Additionally, some companies must comply with security-conscious businesses compliance regulations (SOC2) or comply with Security Council standards (PCI). Access control systems provide quick and convenient entree or exit to authorized individuals, as well as audit trailing, real-time monitoring, remote accessing, and restriction of entry to unauthorized individuals.

Access control systems can monitor a great number of access points in a building and around its perimeter, including facilities, doors, electronic gates, locks and cylinders, workstation access, data center racks, printer access, furniture and cupboards, and letter boxes as well as lockers. The system can provide sophisticated security by controlling entrances and exits or do a simple task like opening a locker. Furthermore, a good access control system excludes intruders and provides real-time event-driven activity monitoring and early warning.

Access control credentials will vary depending on the level of security and the relevance to the job. In a more secure area like a data center, security requirements are increased; users require a combination of credentials, for instance, a proximity card and a biometric reader. In addition, the choice of biometric reader will be considered carefully, based on the error rates that can emerge, like FAR, FRR, accuracy, and anti-spoofing capabilities, such as impersonation and counterfeiting (Araújo et al. 2005). Furthermore, additional scrutiny is needed if the system is operating in a high traffic area, like a hospital or other environment that needs to be hygienic and safe for employees and visitors. The use of antimicrobial material like silver is known to reduce the level of harmful microbes. Adding materials like silver to high-touch surfaces like handles and shared devices can help prevent the spread of bacteria and reduce the rate of hospital-acquired infections (Salto Systems n.d.).

Credential Authentication and Functionality

When an individual's credentials are presented and verified, the system grants them access. Each access control system uses different methods to authenticate users. According to Stalling and Brown (2008), there are four general means of authenticating a user's identity:

- **Something the individual knows**: Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions.
- **Something the individual possesses**: Examples include electronic keycards, smart cards, and physical keys. This type of authentication is referred to as "token."
- **Something the individual is (static biometrics)**: Examples include recognition by fingerprint, retina, and face.
- **Something the individual does (dynamic biometrics)**: Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm (p. 75).

An example of a secure credential is a combination of a proximity card (*something the individual possesses)* and a PIN (*something the individual knows)*. This is an illustration of a 2FA or two-factor authentication.

Before the user's credentials can be presented and verified, the administrator must enroll the user into the system. First, administrator enters the user's information into a database table. The database contains fields such as identification number, name, title, department, street address, city, and telephone number. Most access control software allows customization, for example, adding more fields, according to a company's requirements and protocols.

Different users require different levels of access. After enrollment, the administrator assigns access points or zones (a cluster of access points) and/or specific time restrictions, if required by the institution's security policy. If the system uses a keypad with a PIN, the system conceals the number from the administrator during the enrollment process. Furthermore, if the access control system uses biometric readers, each person's biometric data is scanned, analyzed, and stored in an encrypted format in a secure database.

After the enrollment process, the user may attempt to access the system. The user presents a credential in the form of a smart card, biometric, or PIN to a digital reader. The reader then forwards the credential to a control panel or controller. The controller receives the request to unlock the relay (the electromagnetic apparatus used as a remote operating switch), which is connected to an access point (door, gate, etc.). Finally, the controller (communicating wirelessly or through a local area network (LAN)) accesses the software. Using distributed intelligence, the controller is fully functional even when the software is not communicating with the hardware, enabling the system to work continuously. It is the software that accesses the server and decides whether to unlock the door. The system uses a web application that contains stored data on a remote data server and utilizes a web browser as a client. If the credentials offered match the name in the database, the controller opens the door. If there is no match, permission is denied, and the reader indicates this with a flashing red light-emitting diode (LED). If access is permitted, the LED light flashes green. The following figure displays a typical access control setup with its components.

The credential transaction shown in the above figure is the simplest form of *authentication* method, single-factor authentication (SFA). The system recognizes that the user requesting access employs only one credentialing method, for example, a username and a password or an access card presented to the reader. For improved security, a two-factor authentication (2FA) or a multifactor authentication (MFA) is employed (NIST n.d.-a). The Paul Sarbanes and Michael Oxley act (Sarbanes-Oxley Act of 2002) and HIPAA require that institutions establish strong internal controls to mitigate risks and protect data centers from data breaches (Gordon et al. 2005; Srinivasan 2014). The 2FA and MFA methods use more than one factor to confirm the identity of a user, thereby improving security. An example of the 2FA method could be an access card as the first credential and a secret PIN or biometric identification as the second credential.

Access Control System Topology and Standards

Access control systems are classified as stand-alone, server-based, or utilizing distributed intelligence. Stand-alone access control provides access in situations with minimal problems, like lack of visibility and control of database activity, lack of remote managing and control of users, limited user capacity, and lack of software and/or no audit trail. Additionally, the user database and enrollment information are stored in the reader. This topology is often chosen for controlling apartment or private office doors that do not require management, have many users, and do not require constant monitoring.

Server-based access control is a client-based system which accesses a database and a server. All data concerning the access control system (enrollment user data, authentication requests, access to history and real-time audit trail) reside on the server. When the reader sends an access request to the controller, the controller then sends the request for authentication to the server; finally, the server's database grants or denies the request.

Distributed intelligence access control allows real-time data exchange between locks and credentials (cards, fobs, etc.). The administrator accesses the software to affirm credentials, access as well as integrate locks, and update, restrict access, or delete a user remotely. Additionally, the administrator can view supporting information in real time, such as audit trails, display times, date, and information about user access or denial. Most modern server-based systems incorporate this technology into wireless locks and credentials like RFID cards and mobile apps. Server-based and distributed intelligence access control systems are usually more expensive and require certified license contractors for installation. Corporations with thousands of users and hundreds of doors and exits purchase these systems. Distributed intelligence access controls are found in high-end apartment buildings and smart houses as well.

Access control systems use the Wiegand electrical data interface protocol for communication among the controller, reader, and credential and refer to this as data encoding among the devices (HID n.d.). More specifically, the Wiegand protocol connects peripheral devices (biometric reader, card) with the access control system. The interface contains three connecting wires: the ground wire and two other data transmissions, identified as Data low/DATA 0 and Data high/DATA 1 (HID n.d.). Contactless smart cards follow ISO/IEC 14443, ISO/IEC 15693, or ISO/IEC 18000 standards, developed by the International Organization for Standardization (ISO n.d.-b) and the International Electrotechnical Commission (IEC n.d.). In addition to the above installation and encoding standards, access control systems are governed by the National Fire Protection Association's (NFPA) regulation 101T Life Safety Code (NFPA n.d.) and the International Building Code (ISO n.d.-a) that specifies the range of use of electromagnetic locks. Finally, for access control systems used at federal facilities, the NIST has developed best practice guidelines for integrating credentials with the physical access control systems (PACS) (NIST n.d.-b).

Security Concerns and Risks

Any software that resides on a network and works alongside a variety of IP-based devices (readers, locks, and controllers) is vulnerable to a variety of attacks. By compromising an access control system, a hacker would not only have access to its database, but could control all access points. The hacker could threaten to leak users' sensitive information, delete access data from users' profiles, and open every door or gate connected to the system unless the institution pays ransom. Many companies that are turning to IP-based access control systems lack awareness and understanding of the security vulnerabilities that can lead to an attack. Another problem is the lack of communication and collaboration among installers, system administrators, and the IT security of the organization. As a result, IT security can overlook issues such as insecure software, firmware, installation of the readers, controllers and wireless locks, unprotected mobile app interfaces, insecure web interfaces, and lack of transport encryption. They may choose to favor convenience over security by simplifying usernames and passwords.

Another issue is that some software manufacturers do not provide follow-up with IT security after installation. Furthermore, some components (readers, locks) come from third-party vendors and run on outdated software/firmware. Hypothetically, an attacker could exploit all the above vulnerabilities to gain access to organization's networks. Hacking techniques include packet sniffers (Wireshark), where a hacker first captures and then analyzes data packets that can be used to obtain information like passwords, and the man-in-the-middle (MITM) attack, where the hacker eavesdrops on the communication between two targets using a separate computer that accepts traffic from each one (Gibson 2009). Security attacks are increasing in quantity and severity every year, and will not lessen, especially when hackers know that organizations will meet their ransom demands.

Conclusion

Physical access control technology has grown tremendously in recent years and is changing how we secure our sites. Wireless solutions, used with a variety of credentials, can secure many things besides doors and gates. Smart homes integrate access controls, a variety of credentials, and a security system, along with closed-circuit cameras and lighting and sound systems, under a single control panel that can be accessed from anywhere in the world. Those using wireless solutions can expect an increase in IT vulnerabilities and data breaches. In the corporate environment, physical access controls, used with fire alarm systems, are becoming critical investments for every organization.

The choice of an access control system should be treated as a long-term capital investment. According to the Technology Acceptance Model (TAM) (Davis 1986, 1989), two factors influence technology adoption, the technology's perceived usefulness and perceived ease of use. Thus, an access control system should be both easy to use and should have the ability to transform the organization. The system must have distributed intelligence and the ability to integrate with other systems, such as closed-circuit cameras, alarms, and fire systems. The system must follow accepted fire and life-safety codes. In addition, the system should be able to expand and handle additional users, devices, and locations within one application. In the age of mobility, users should be able to gain access to and monitor the system using credential and monitoring apps on their mobile devices.

Credentials should offer convenience and ease of use and of course should be cost-effective. Biometric authentication credentials must be evaluated based on accuracy factors, such as FAR, FRR, and identification rate. In some cases, a mobile phone app using Bluetooth or near-field communication (NFC) may be used as a credential for communicating between the mobile phone and the lock. Furthermore, from a security perspective, the system should be able to accept smart credentials like encrypted RFID card technology and biometric readers. Finally, one of the most important security factors is that the manufacturers must provide critical software updates, including security and firmware updates, on a regular basis, in conjunction with the IT department of the organization. Communication between the vendor, manufacturer, and IT department and systematic training of administrators are critical for the success of the system. Any system cannot survive and be effective unless the human element is handled successfully. In today's digital world of increasing cybersecurity awareness, it is important to combine both *physical and logical access controls* in the effort to restrict, analyze, and protect access to network data and physical locations.

Cross-References

- ▶ Airport Security: Procedures in Secured Areas for TSA and Private Security
- ▶ Biometrics
- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Physical Security: Best Practices

References

Access controlled egress doors building code. (n.d.-a). Retrieve from 2018 International Building Code https://codes.iccsafe.org/public/document/IBC2018 and Chapter 10 - Means of Egress https://codes.iccsafe.org/public/document/IBC2018/chapter-10-means-of-egress

Araújo, L. C., Sucupira, L. H., Lizarraga, M. G., Ling, L. L., & Yabu-Uti, J. B. T. (2005). User authentication through typing biometrics features. *IEEE Transactions on Signal Processing, 53*(2), 851–855.

Bacco, E. M., Prinzivalli, D. P., & Collins, A. T. (2017). U.S. *Patent No. 9552684B2*. Washington, DC: U.S. Patent and Trademark Office.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Ph.D. dissertation. Massachusetts Institute of Technology, Boston.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

de Vries, M., Cross, N., & Grant, D. P. (Eds.). (1993). *Design methodology and relationships with science*. Dordrecht: Kluwer.

Encyclopedia Britannica, Lock Security. (n.d.). Retrieve from https://www.britannica.com/technology/lock-security

Gibson, D. (2009). *CompTIA security+: Get certified get ahead SY0-201 study guide*. Charleston: BookSurge Publishing.
Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal, 21*(3), 1.
HID White paper. (n.d.). Understanding Card Data Formats. Retrieve from https://www.hidglobal.com/sites/default/files/hid-understanding_card_data_formats-wp-en.pdf
International Organization for Standardization (ISO). (n.d.-b). Retrieve from https://www.iso.org/home.html
Life Safety Code, National Fire Protection Association (NFPA). (n.d.). Retrieve from http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=101
Nemeth, C. P. (2017). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.
Norman, T. L. (2011). *Electronic access control*. Waltham: Elsevier.
Salto Systems. (n.d.). Antimicrobial Access Control Systems. Retrieve from https://www.biocote.com/partners/salto/
Srinivasan, S. (Ed.). (2014). *Security, trust, and regulatory aspects of cloud computing in business environments*. Hershey: IGI Global.
Stallings, W., & Brown, L. (2008). *Computer security: Principles and practice*. Saddle River: Pearson Education.
The International Electrotechnical Commission (IEC). (n.d.). Retrieve from http://www.iec.ch/.
The National Institute of Standards and Technology (NIST). (n.d.-a). Back to basics: Multi-factor authentication (MFA). Retrieve from https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.
The National Institute of Standards and Technology (NIST). (n.d.-b). Recommendation for the Use of PIV 25 Credentials in Physical Access Control Systems. Retrieve from https://csrc.nist.gov/csrc/media/publications/sp/800-116/rev-1/draft/documents/sp800_116_r1_draft.pdf.
The Sarbanes–Oxley Act. (2002). Pub. L. 107–204, 116 Stat. 745.

Further Reading

Bluetooth technology standards. Retrieve from https://www.bluetooth.com/.
Health Insurance Portability and Accountability Act. (1996). Pub. L. No. 104-191, § 264, 110 Stat.1936. Retrieve from https://www.hhs.gov/hipaa/index.html
Security Council standards (PCI). Retrieve from https://www.pcisecuritystandards.org/.
Security-conscious businesses (SOC2). Retrieve from https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.
The Joint Commission. An independent, not-for-profit organization. Retrieve from https://www.jointcommission.org/.
Wi-Fi alliance. Retrieve from https://www.wi-fi.org/.

Physical Security: Methods and Practices

Adam D. Williams
Center for Global Security and Cooperation, Sandia National Laboratories, Albuquerque, NM, USA

Keywords
Physical security · Detection · Delay · Response · Design

Definition

Physical security methods and practices are those systematic plans and actual uses of countermeasures applied to prevent unauthorized access to, and protect against malicious acts upon, critical assets.

Introduction

Physical security – despite the simplistic refrain that all it consists of is "gates, guards, and guns" – is not a "one-size-fits-all" enterprise. Rather, it consists of the use of active and passive measures to protect critical assets from adversary or criminal activities by preventing unauthorized access to critical assets – be they personnel, buildings, geographic areas, or equipment (see ▶ "Insider Threat" for further discussion). According to the US Department of Defense, physical security is defined as "That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft" (2016, p. 185). In addition,

SAND9629J Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the US Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

physical security seeks the "protection of Federal employees and private citizens who within and visit U.S. government-owned or leased facilities" (Interagency Security Council 2015, p. iii).

After describing high-level physical security goals, the rest of this entry describes how two mechanisms can support the completion of such goals for critical assets. The first consists of *physical security methods*, or the systematic planning related to physical security countermeasures implemented for protecting critical assets (e.g., systems-engineering design frameworks). The second encompasses *physical security practices*, or how physical security countermeasures are used to protect critical assets (e.g., facility-specific access control procedures).

The Goals of Physical Security

To evaluate the effectiveness of related methods and practices, it is necessary to understand the goals of physical security. Physical security can best be measured by the ability of *countermeasures* –technologies, procedures, and individuals – to interact in support of all efforts to identify, slow, and neutralize any adversary or criminal action against critical assets (Garcia 2008; Interagency Security Council 2015). More simply put, the "theory and application of physical [security], include the functions of deterrence, *detection*, *delay*, and *response*" (Interagency Security Council 2015, p. 19).

Detection, as a physical security goal, relates to all countermeasures that communicate the occurrences of an adversary or criminal activity against an asset is occurring. Examples include guard patrols observing an individual climbing a perimeter fence or a motion sensor indicating movement inside a locked vault. The detection goal includes the process by which observations of undesired actions (e.g., surveillance and monitoring) are analyzed (e.g., detection and assessment) and lead to decisions to initiate additional protection actions. When concentrated farther away from critical assets, detection countermeasures are more effective and efficient because they provide additional time for more accurate assessment and for supplementary protection actions to be taken. Detection effectiveness is generally described as the likelihood that the selected collection of related countermeasures are able to adequately identify the presence of adversary or criminal activities threatening critical assets. (For additional discussion on related topics, see ▶ "Intrusion Detection Systems," ▶ "Physical Security: Interior Applications," or ▶ "Physical Security: Video Surveillance, Equipment, and Training.")

Delay, as a physical security goal, includes countermeasures employed to increase the physical resources, intellectual capabilities, and time necessary for an adversary or criminal action to be successful. Common examples of delay countermeasures include cement bollards to prevent vehicle access or enhanced locking mechanisms on entrances to sensitive buildings. Countermeasures selected and implemented to support delay goals seek to insert additional time into adversary or criminal activities for other protection actions to be successfully deployed. Delay-related countermeasures are most effective and efficient when they occur after detection and are concentrated closer to critical assets. (Perhaps the quintessential example of the "delay after detection" mantra is illustrated in a scene from the 1994 film *The Shawshank Redemption*. In the film, Andy Dufresne spent years slowly chipping away at his cement-walled prison cell. He was able to eventually dig a hole large enough to facilitate his escape – completely unbeknownst to the prison guards or warden. In this example, even the delay of multiple-foot-thick prison cell walls are negated because there was no forewarning – or detection – of the malicious act.) The ability to achieve delay-related goals is described as the additional time provided by extra physical, temporal, or cognitive burdens placed on adversary or criminal activities against critical assets.

Response, as a physical security goal, incorporates countermeasures for neutralizing adversary or criminal activities against critical assets by killing, capturing, or causing them to flee. Examples include using onsite guard personnel to cordon off a specific area to contain the perpetrators or the arrival of an offsite, armed

local law enforcement agency. Countermeasures supporting response goals can include providing improved equipment, requiring advanced tactical training, enhancing communications, or moving forces closer to critical assets. Timely and appropriate response, in general, is most effective and efficient when coordinated with early detection and sufficient delay by other physical security countermeasures. Response effectiveness is commonly described as the speed and efficiency with which appropriate response personnel – most often agencies with national or local authority to carry weapons – are able to arrive and neutralize adversary or criminal activities against critical assets. (For additional discussion on related topics, see ▶"Security Guards: Academic and Training Programs" or ▶"Security Guards: Authority and Power.")

Taken together, these physical security goals aim to prevent interruptions to the benefits provided by critical assets – arguing that there is an inherent need for alignment between physical security goals and desired asset operations. Therefore, the level to which countermeasures independently and interdependently operate to achieve high-level physical security goals *within* the context of normal facility operations will determine the overall effectiveness of being able to protect critical assets. According to the US Interagency Security Council (ISC), it is important to "articulate how a holistic and comprehensive physical security program contributes to the success of the agency and its mission" (Interagency Security Council 2015, p. 20). Achieving physical security goals can be most efficiently and effectively achieved by leveraging insights from well-known physical security methods and practices.

Overview of Physical Security Methods

Successfully detecting, delaying, and responding to adversary or criminal activities to protect critical assets require strategic thought, tactical understanding, and rigorous evaluation. In response, physical security *methods* can be defined as systematic planning processes to identify, select, and arrange physical security countermeasures to protect critical assets from threats. Navigating such influences as normal asset operations, natural terrain, and architectural designs on physical security performance requires an emphasis on balance identifying, selecting, and arranging countermeasures. While various methods exist for identifying, selecting, and arranging physical security countermeasures to protect critical assets, this entry uses two examples to crystallize this concept. The first is the *design evaluation and process outline*, which was created at Sandia National Laboratories for the protection of various US Department of Defense and US Department of Energy critical assets. The second is *crime prevention through environmental design*, which evolved from the "defensible space" concept that emerged from the union of criminology and architecture domains in the 1970s (Ray 1971).

The Design Evaluation Process Outline (DEPO) builds generic systems engineering concepts for its systematic planning for physical security. DEPO is popularly considered the current standard for security analysis at nuclear facilities (Garcia 2008). The DEPO methodology consists of the following key steps (Garcia 2008):

- Characterize the facility (e.g., *defining its mission*)
- Identify the undesired events and critical assets (e.g., *identifying assets as theft or sabotage targets*)
- Determine potential consequences of undesired events (e.g., *defining facility damage, or health effects)*
- Define threats to the facility (e.g., *identifying anticipated adversary capabilities*)
- Analyze security system effectiveness (e.g., *evaluating performance of physical security countermeasures*)
- Estimate the risk (e.g., *determining how well the physical security countermeasures mitigate adversary activities)*
- Compare this risk to the *acceptable* risk level from the competent authority and:
  - If sufficient, complete the (re)design of physical security countermeasures.
  - If insufficient, suggest (and re-evaluate) physical security countermeasure upgrades.

The DEPO method argues that the "detect, delay, and respond" paradigm fully describes the necessary functions of strong physical security (Garcia 2008). As a physical security method, DEPO seeks to between the accepted level of risk (e.g., the likelihood of successful adversary or criminal action) and physical security upgrade impact to facility budget and operations. To do so, DEPO shares a philosophical foundation with popular probabilistic risk assessment approaches to safety and arranges countermeasures to make adversary tasks more complex and take longer to complete. According to DEPO, extending the adversary or criminal timeline improves the ability of countermeasures to achieve physical security-related goals.

To this end, DEPO describes how well an arranged collection of physical security countermeasures to achieve a defined ability of defeating a specific adversary along a specific attack path. More specifically, this method describes a conditional probability that adversary or criminal activities will be interrupted in time for them to be neutralized for how well detection and delay goals are achieved. Similarly, DEPO describes a conditional probability that, once interrupted, adversary or criminal activities are neutralized for how delay and response goals are achieved. Ultimately, the DEPO method produces an overall description – called the system effectiveness – of the ability of a given collection of physical security countermeasures to achieve detection, delay, and response goals to protect critical assets against malicious acts. (DEPO uses the formula $R = P_A * (1-P_E) * C$ to determine system effectiveness, where P_A is the assumed probability of attack, C is a quantitative approximation of qualitative consequence descriptions, and P_E is the physical security system effectiveness. To mitigate the difficulty of predicting adversary actions (P_A), DEPO best practices set $P_A = 1$ to simplify the equation to $R_C = (1-P_E) * C$. With physical security now described as a conditional probability, P_E is defined as the product of the probability of interruption (P_I) and the probability of neutralization (P_N), where P_I and P_N are nested, conditional probabilities related to physical security countermeasure performance.)

A second example of a physical security method is Crime Prevention through Environmental Design (CPTED). This method is based on the argument that urban form – including landscapes, buildings, and traffic flow patterns – can be used to reduce criminal activity. This multidisciplinary approach leverages concepts from social, behavioral, psychological, and biological explanations for what causes criminal and malicious behavior. More specifically, CPTED is:

> A process for analyzing and assessing crime risks in order to guide the design, management, and use of the built environment (and products) to reduce crime and the fear of crime and to promote public health, sustainability and quality of life. (Cozens and Love 2015, p. 14)

CPTED, ideally, is implemented during design phases, because they offer the most flexibility and control over potential changes in the environment. Cozens & Love (2015) summarize this method in terms of seven physical and four social strategies. These physical strategies include creating a sense of ownership to protect an asset (e.g., "territorial reinforcement"); observing various activities in an area around an asset (e.g., "surveillance"); maintaining appearance to transmit positive signals about an asset (e.g., "image"); limiting entrance to, or contact with, an asset (e.g., "access control"); promoting high levels of desired activities around assets (e.g., "legitimate activity support"); increasing the physical difficulty of accessing an asset (e.g., "target hardening"); and using the influence adjacent "safe zones" to protect assets (e.g., "geographical juxtaposition"). Similarly, the four social strategies, according to Cozens & Love (2015), include building a mutual respect among members in a local community (e.g., "social cohesion"), coordinating activities among members in a local community (e.g., "community connectivity"), sharing a sense of place between members of a local community (e.g., "community culture"), and understanding the finite ability to support certain community activities (e.g., "threshold capacity"). CPTED has a long history of being used as a method to reduce crime in community spaces (Cozens and Love 2015) – which provides examples of how its use for systematic planning helps

achieve physical security goals. For example, CPTED's argument that revitalizing dilapidated portions of neighborhoods will eliminate opportunities to conceal criminal activities is similar to the physical security goal of detection. Similarly by restricting access, delay is demonstrated in CPTED-based redesigns of walking paths to limit entranceways into public space. The social strategies listed above also serve to better incorporate relevant law enforcement agencies into CPTED-based plans which results in increased familiarity and trust with the community. This can cause more effective and more efficient prevention of crime by these law enforcement agencies and directly serves the response physical security goal. As a method, CPTED "continues to represent an attractive option for individuals, communities, local, state and national governments and international organizations alike" (Cozens and Love 2015, p. 14) for leveraging to achieve physical security goals for critical assets.

Additional physical security methods also exist. One other popular method, known as "defense-in-depth," argues for using combinations of physical security countermeasures (each considered insufficient to meet physical security goals on their own) in concentric layers to enhance physical security performance. For example, using a chain-link fence and ring of tall shrubbery around a public space combines the robustness of the former with the opacity of the latter to enhance the overall physical security of the space. The concept of a "graded approach" – which argues for appropriately matching selected and arranged physical security countermeasures to facility operations, anticipated threats, and potential consequences – is another systematic planning process for physical security. Consider, for example, the countermeasures employed to protect a remote power substation in the rural USA. Midwest will look different than those for a nuclear power plant near a metropolitan area for the same anticipated threat because of the differences in operations and potential consequences. Despite the common goals of detecting, delaying, and responding to adversary or criminal activities to protect critical assets, physical security methods provide systematic planning processes to avoid a "one-size-fits-all" physical security mentality.

Actual Application(s) to Protect Assets from Threats: Physical Security Practices

In physical security, systematic planning should be augmented by a deeper understanding of (and expectations for) the patterns that describe regular application of physical security countermeasures. In other words, where methods illustrate systematic planning processes for physical security countermeasures (e.g., actions taken during the *design* of physical security), practices describe how such countermeasures are routinely *used*. Physical security *practices*, then, can be defined as the behavioral patterns of how individuals interact with physical security countermeasures to achieve asset protection goals. Therefore, the ability to achieve physical security goals is enhanced with a deeper understanding of such behavioral patterns, and, while many exist, two are described in more detail to illustrate the importance of this concept.

Successful physical security is predicated on the having an accurate understanding of the current conditions impacting countermeasure performance and the asset they are intended to protect. *Surveillance* is a key physical security practice that relates to countermeasures are used to make observations that inform this understanding of current conditions influencing asset protection. Traditionally, surveillance relates to targeted, close observation of suspicious (or, expected to be suspicious) activities – surveilling an employee suspected of tampering with a bank vault, for example. There are different kinds of observations, however, that can inform knowledge of the current conditions impacting countermeasures. Monitoring, for example, describes efforts for broad observations of critical assets at regular time intervals, often as a quality control mechanism. Consider cameras aimed at the entrance door to a bank, for example. Another type – assessment – describes the ability to distinguish between non-malicious and malicious intent for unexpected or unanticipated observations. Ultimately, assessments aim to identify whether the

observation was a tumbleweed blowing into the bank lobby or an adversary or criminal activity.

As a physical security practice, surveillance supports both DEPO- and CPTED-based countermeasure designs to achieve high-level physical security goals. In DEPO, various technical- and human-based countermeasures are identified and implemented to improve the observation and communication of unexpected activities to support the method's emphasis on assessed detection (Garcia 2008). Common examples include roving guard patrols along a facility's perimeter and closed-circuit television (CCTV) systems. Similarly, CPTED argues that the ability (and the *perceived* ability) for regular observations of activities in public spaces deters criminal acts for fear of exposure and attribution. CPTED-specific examples include street design (e.g., one-way traffic flows), the location of building windows (e.g., some should face the back alley), and CCTV (Cozens and Love 2015). Whether performing under the specific parameters of surveillance, monitoring, or assessment, physical security is enhanced when countermeasures improve the quantity and quality of observations on conditions related to protecting assets.

In addition to having early warnings of potentially adversary or criminal activities, physical security is also enhanced by efforts to purposefully restrict proximity to (or contact with) critical assets. This physical security practice distinguishes between who does (and who does not) have authority to access a critical asset. Called *access control*, this practice includes behavioral patterns that use countermeasures to limit the ability for close proximity or contact with critical assets. Related practices include more formal efforts like background investigations commonly used for US government jobs requiring a national security clearance and informal mechanisms like neighbor-based identification of "strangers" in the community. Access control practices also include discriminating based on the type of access allowed to support achieving physical security goals. For example, access to a bank's vault can range from bank customers being escorted to their safety deposit boxes to bank employers entering the vault unescorted during business hours to bank managers having the codes to open the vault during nonbusiness hours. Asset protection, then, can be enhanced by practices that restrict the number of people or the type of proximity to assets that are permitted.

Access control practices, like surveillance, supports DEPO- and CPTED-based countermeasures to help achieve high-level physical security goals. Related practices include both technological and procedural mechanisms to (at best) eliminate or (at worst) reduce unauthorized access to protected assets. Common DEPO-based applications of access control include the use of identification badges – from simple visual inspection to electronic examination to biometric verification. Likewise, one of the key CPTED strategies centers on access control, more specifically emphasizing both natural and man-made uses of "spatial definition to deny access to potential targets" (Cozens and Love 2015, p. 5). Using landscape features like steep terrain or creeks to locate entranceways are traditional CPTED-related approaches to access control, but more recent practices include using mechanical locks and cages to deny unauthorized proximity to assets. In both DEPO- and CPTED-related instantiations, access control practices support achieving high-level delay goals. When used to support surveillance efforts (e.g., alerting when an employee suspected of malicious intent attempts access to an asset), access control can also help achieve detection goals. These practices can also support high-level physical security response goals, particularly when utilized in a forensic or investigatory role.

While surveillance and access control were highlighted in this entry they are not the only physical security practices to consider in achieving physical security goals. Another visible physical security practice is employing dedicated, on-site guard personnel. Such personnel can range from contracted personnel who focus on small theft prevention (as in many US retail stores) to (un)armed individuals who focus on slowing criminal activities (as in many US commercial banks) to armed personnel with paramilitary training (as in many US nuclear power plants). Another popular physical security

practice relates to the use of protection zones, where different levels of countermeasures are located to protect different types of assets. Most clearly related to the aforementioned "defense-in-depth" physical security method, this practice places more valuable assets in zones that require more robust countermeasures, with the tendency of placing the highest value assets in the center of a concentric set of protection zones. An example of clear protection zones are those around nuclear power plants, but similar practices can be seen in more common organizations like airports where increasingly robust countermeasures protect access to the terminal(s), aircraft, tarmac, and air traffic control towers. Taken together, this section demonstrates the important role of how regular patterns of using countermeasures support systematic planning processes to achieve physical security goals to protect critical assets.

Conclusions

Physical security methods and practices must continually adapt to changing and expanding challenges into opportunities for better critical asset protection. Consider the natural tension between physical security countermeasures and the operational focus of critical infrastructure, like the difficulty in balancing between the resources spent on attempting to detect weapons entering an airport and the need for airports to process thousands of people an hour. Here, coupling a focus on preventing interruptions to normal operations with detection, delay, and response goals provides the opportunity to develop new systematic planning processes and patterns of behaviors to protect critical assets. Another challenge is confusing "threat" (or, those aspects of physical security that *cannot* be controlled) and "vulnerability" (or, those aspects of physical security that *can* be controlled). Threats to physical security can either be natural (e.g., floods, fires, hurricanes) or intentional (e.g., terrorist or criminal acts), whereas vulnerabilities are faults within countermeasures that can be addressed (and resolved) with physical security methods and practices. Further, new and evolving threats should be used as drivers for innovation in physical security methods and practices. One last challenge is the increasing digitization of physical security countermeasures (e.g., controllers of physical countermeasures or networked countermeasure system designs). This, in turn, provides the opportunity to better incorporate key cyber security and information protection strategies into physical security methods and practices. Ultimately, combining and leveraging the benefits of well-known – and developing new, innovative – physical security methods and practices can help overcome these challenges to ensure that critical infrastructure assets are protected and able to support their role in society.

Cross-References

- ▶ Insider Threat
- ▶ Intrusion Detection Systems
- ▶ Physical Security: Interior Applications
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Security Guards: Academic and Training Programs
- ▶ Security Guards: Authority and Power

P

References

Cozens, P., & Love, T. (2015). A review and current status of crime prevention through environmental design (CPTED). *Journal of Planning Literature, 30*(4), 393–412.

Garcia, M. L. (2008). *The design and evaluation of physical protection systems* (2nd ed.). Boston: Butterworth-Heinemann.

Ray Jeffery, C. (1971). *Crime prevention through environmental design*. Beverly Hills: Sage Publications.

U.S. Department of Defense (2016). Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1–02). https://fas.org/irp/doddir/dod/jp1_02.pdf.

U.S. Interagency Security Council, Department of Homeland Security (2015). Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide. https://www.dhs.gov/sites/default/files/publications/isc-planning-managing-physical-security-resources-dec-2015-508.pdf.

Further Reading

Relevant Standards within the United States Code (U.S.C.) and the Code of Federal Regulations (CFR) for physical security can be located by searching for specific U.S. government entities.

Cozens, P. (2014). *Think crime! Using evidence, theory and crime prevention through environmental design (CPTED) for planning safer cities*. Quinns Rock Perth: Praxis Education.

Garcia, M. L. (2005). *Vulnerability assessment of physical protection systems*. Boston: Butterworth-Heinemann.

Physical Security: Video Surveillance, Equipment, and Training

Anthony Morgan[1] and Christopher Dowling[2]
[1]Serious and Organised Crime Research Lab, Australian Institute of Criminology, Canberra, ACT, Australia
[2]Australian Institute of Criminology, Canberra, ACT, Australia

Keywords

Video surveillance · Closed circuit television (CCTV) · Crime prevention · Public space · Policing · Security

Definition

The use of video surveillance for physical security refers to closed circuit television (CCTV). CCTV is used as a generic term to describe one or more video cameras that are connected via a closed system to a central television monitor or recording device (Ratcliffe 2011). The terms video surveillance and CCTV are used interchangeably in this entry.

Introduction

Video surveillance systems are commonly employed as a physical security measure in many western countries. The number of cameras being used in the United Kingdom – an early leader in embracing the use of CCTV, through the support of the Home Office (Armitage 2002) – is estimated to be between two and six million (British Security Industry Association 2013; Gerrard and Thompson 2011; McCahill and Norris 2002). Almost half of all US police departments, and as high as 90% for large departments, use video cameras for surveillance of public areas (Reaves 2015). Several large US cities have invested heavily in video surveillance; for example, Chicago now has more than 30,000 cameras in public areas (Williams 2018). Australia also has a significant investment in public space CCTV by local councils. Between 2005 and 2014, there has been a sixfold increase in the proportion of councils responsible for the installation and monitoring of public space video surveillance systems that use federal, state, and territory government funds (Hulme et al. 2015). Meanwhile, the largest growth in CCTV has been observed in Asia. Industry estimates have placed the number of cameras in China at approaching 200 million, with plans to grow this number significantly in the short term (Mitchell and Diamond 2018) as part of a larger surveillance network (Liang et al. 2018).

Evidence supports the finding that CCTV makes an important contribution to public safety and helps guide decisions by private and public security managers about when, where, and how CCTV is used. This entry begins by exploring the different features of video surveillance systems, followed by a description of how CCTV is meant to enhance public safety. The data evaluating the effectiveness of CCTV is briefly reviewed, including support for features that seem to be key to security management. Lessons for the effective use of CCTV as a physical security measure, including equipment and training, are then outlined.

Characteristics of Video Surveillance Systems

The size of the global video surveillance market has been estimated at over $30 billion (BIS Research 2018). Video surveillance systems

comprise several main elements, including cameras and lenses, monitors, recording devices and video storage, the hardware connecting each of these, and relevant supporting infrastructure. However, the configuration of video surveillance systems can vary widely from a single camera to many thousands of connected cameras or from simple inexpensive home installations to large-scale multi-million-dollar public space networks. In addition to private residences, CCTV systems are utilized in a range of settings where there may be security risks, including retail and commercial premises, financial institutions, public transport, car parks, city centers, and entertainment precincts and venues.

Cameras may be stationary, with a fixed field of vision, or move according to a pre-programmed pattern of movement, while pan, tilt, and zoom (PTZ) cameras allow for operators to control the movement of cameras and focus on targets of interest. PTZ cameras have become increasingly common, particularly in those systems that are monitored by camera operators, while pre-programmed and stationary cameras are often criticized for failing to capture important moments or features of an incident (La Vigne et al. 2011). There has also been an increase in the use of mobile cameras, which allow video surveillance to be deployed in known hot spots.

Contemporary video cameras use digital technology, although they may be connected to existing analogue cameras, particularly in those situations where an existing network is being expanded or upgraded. Digital cameras offer significant advantages over analogue cameras but, even then, can vary in terms of image capture and resolution. This is influenced by a wide range of factors, including the type and quality of the camera and camera lens, the lighting that is available (and whether the camera adjusts to day- or nighttime and is able to perform well in low-light situations), the type and level of digital video compression for image transmission and storage, and the resolution, scaling, and capabilities of the display device. Fundamental to the performance of a video surveillance system in terms of capturing a high-quality image are the type and features of the camera lens; there is little capacity to compensate for a poor-quality lens with other components of the system.

Cameras may be connected via cabling, via wireless connectivity, and increasingly, via Internet protocol networks. Internet protocol cameras have grown in popularity, due to their capacity to provide high-quality image resolution at a comparatively low cost. Cameras are usually connected to a central monitor, or bank of screens, while digital technology allows for footage from multiple cameras to be recorded simultaneously. Footage is usually recorded on digital video recorders or network video recorders, the size of which will be influenced by the quality of video recorded, as well as the length of time (i.e., how many days) the footage needs to be retained before being recorded over. Many systems still rely on write-once, read-many media – such as CDs and DVDs – for video storage, but there is a shift toward secure network storage, particularly for larger systems. In avoiding the need to handle storage disks, which can be cumbersome, network storage is more readily scalable as a network or storage requirements grow (Space and Naval Warfare Systems Center Atlantic 2013).

Camera systems may be live monitored, passively monitored, or unmonitored. Monitoring requirements will dictate the number and type of monitors (e.g., display resolution, size, layout) that are used to view images. The major advantage of monitored systems is the ability to detect incidents as they occur and to deploy security or police shortly thereafter. This has significant resource implications, including to establish control rooms and provide ongoing staffing, and requires effective communication between camera operators and frontline responders. Research suggests that most systems are not monitored and that the proportion of public space systems monitored has fallen as the number of systems has grown (Hulme et al. 2015), and most criminal incidents that occur in locations with video surveillance are not detected by CCTV operators (Piza et al. 2014b). However, this varies by context, with larger public infrastructure systems – which might be supported by dedicated security or direct communication with police – more likely to include a monitoring

capability (e.g., public transport surveillance networks; see Ashby 2017; Morgan and Coughlan 2018). Footage that is not monitored may still be recorded – and stored for a minimum length of time – which allows investigators and other users to access footage at a later date. However, not all operators routinely record footage, usually because of resource implications.

Importantly, video surveillance systems are rarely used in isolation of other public safety measures. Instead, they are used in combination with access control measures, street lighting, crime prevention through environmental design, and the deployment of security guards. These other forms of public area surveillance are effective crime prevention measures themselves (Welsh et al. 2015). Similarly, police use CCTV alongside a raft of other technology, while video surveillance in law enforcement settings also includes body-worn cameras, automatic number plate recognition systems, and facial recognition. In fact, most significant advances in contemporary policing revolve around the introduction of new technologies for law enforcement. Although this entry focuses on video surveillance, it must be understood that this is often implemented as part of a larger strategy.

Potential for CCTV to Reduce Crime and Improve Public Safety

According to Gill and Spriggs (2005), there are several possible mechanisms through which video surveillance may help to reduce crime and improve public safety. Although there has been little attempt to empirically test these mechanisms, they are important because the way CCTV works has implications for how systems are designed and implemented (see ▶ "Physical Security: Best Practices" and ▶ "Physical Security: Video Surveillance, Equipment, and Training" in this encyclopedia). These mechanisms are also helpful in interpreting the research findings that follow.

The most obvious of these mechanisms, and the mechanism that is most commonly assumed, is general deterrence. Potential offenders may be deterred by the presence of video surveillance because it increases their perceived risk of getting caught. This assumes that offenders are aware that cameras are installed in the area – which requires cameras and signage be visible – and believe they are being monitored or that footage is used to identify offenders and that the risk of being apprehended outweighs the potential rewards associated with committing crimes in areas with surveillance cameras installed.

Several other mechanisms are possible. These include that video surveillance increases the actual likelihood of an offender being apprehended and processed through the criminal justice system, which reduces their likelihood of repeat offending through incapacitation or specific deterrence. Given the high proportion of offenses committed by repeat offenders, often against the same targets, this seems plausible (Grove and Farrell 2012), particularly in high-crime areas. In areas where quality CCTV footage is collected and stored, and partnership arrangements between CCTV operators and police exist to facilitate footage retrieval, the ability to identify and prosecute offenders should be enhanced. Video surveillance systems that are monitored may support the rapid deployment of police and security staff to incidents when they occur, or when individuals are acting suspiciously, which can interrupt offenders and prevent crime from occurring or escalating.

Other mechanisms may be more indirect. Video surveillance is often installed with the goal (usually alongside crime prevention) of improving perceptions of safety because of how it might influence people's perception of the space. The presence of video surveillance devices may signal to potential users of public space that the area is safe, making them less likely to worry about security risks and more likely to visit, and the increased presence may result in increased informal or natural surveillance from people who may act as capable guardians, a known deterrent to offenders. Conversely, the presence of visible CCTV may indicate to people using the space that there is a security risk, encouraging those who are more security-minded to take additional precautions.

Finally, video surveillance may also have potential negative consequences, which could lead to an increase in crime. It is possible that recorded crime will increase, not because of actual changes in crime, but because CCTV increases the number of crimes that are detected by police (Winge and Knutsson 2003). Another possibility is that police, security personnel, and members of the community become less vigilant in the presence of video surveillance, because they believe would-be offenders will be deterred or that, if something were to happen, those monitoring the cameras will respond quickly to intervene. It is also possible that CCTV will lead to a decrease in natural surveillance, because people who do not like the idea of being captured on camera avoid the area. Whether the concerns raised in relation to privacy implications of public space surveillance actually lead to changes in behavior in public spaces has not been subjected to any empirical analysis.

There are other uses for video surveillance, including monitoring of industrial operations, traffic monitoring, counter terrorism, and emergency management, which are important but outside the scope of this entry. In summary, video surveillance has the potential to deliver several benefits relating to physical security in public spaces, including reduce crime, improved community safety, more responsive policing, and better investigative outcomes. This entry now turns to discussing the evidence regarding the efficacy of video surveillance in each of these domains.

Effectiveness of CCTV

There is now a very large body of high-quality research that has evaluated the effectiveness of video surveillance, more so than just about any other situational crime prevention measure. Most of this research has focused on the crime prevention effects of CCTV, particularly in the United States and United Kingdom and increasingly other parts of Europe. A recent systematic review of 40 years of evaluations provides the best of evidence of the effectiveness of CCTV as a crime prevention measure, as well as the circumstances under which it works most effectively (Piza et al. 2019). To be included in this review, studies must have measured crime before and after the installation of CCTV (allowing analysis of crime trends), including in the area with cameras and a similar location without cameras installed. This qualification allowed researchers to determine whether any changes in crime could be attributed to the intervention, in this case CCTV, or whether it reflected broader trends or was the result of some other cause.

Overall, Piza et al. (2019) analyzed 80 high-quality studies and found CCTV was associated with a modest, but significant, reduction in crime. Consistent with earlier reviews (e.g., Welsh and Farrington 2009), they found that CCTV was most effective in reducing crime in car parks, primarily thefts from motor vehicles. However, there was also evidence of a positive impact in residential settings. Drug crime, namely, drug selling, had the largest overall effect size – albeit in a smaller number of studies – suggesting drug sellers may be deterred by the presence of security cameras. CCTV was less effective in other settings, such as city centers, and had no impact on violent crime. This is most likely because of the impulsive nature of violence occurring in public spaces (Felson and Massoglia 2012), as well as the fact that many offenders are likely to be affected by alcohol and drugs (Ratcliffe 2011). These factors together likely undermined the deterrent effects of visible security measures, such as CCTV cameras. In circumstances in which crime had been reduced, there was little evidence of displacement, meaning that the crime problem had not simply moved somewhere else, a finding which is consistent with the broader literature on situational crime prevention (Johnson et al. 2014).

There is much less evidence that video surveillance has a positive effect on perceptions of safety. Lorenc et al. (2013) conducted a systematic review of environmental responses to fear of crime, finding limited evidence in support of CCTV. Some studies have produced no effect or small positive effects, whereas others have shown that the installation of CCTV made people feel unsafe. One explanation for these

mixed results is that other factors – such as prior victimization – significantly influence how safe people feel in public spaces despite the presence or absence of physical security measures, such as video surveillance.

While there is an abundance of research into the crime prevention effects of CCTV, the main reason police invest in video surveillance is offender detection and apprehension (Ratcliffe 2011). A small number of studies have shown that CCTV can have a modest effect on the deployment of police. In their Australian study, Wells et al. (2006) conducted 100 h of observation in a CCTV control room, where 181 incidents were viewed by camera operators, resulting in 51 arrests; however, only seven of these arrests were the direct result of the camera network. In another study, Piza et al. (2014b) found that incidents detected using monitored CCTV were more likely than calls for service to result in an offender being apprehended. But this effect was atypical and became even less common as the system increased in size because of the concomitant strain on resources to monitor the footage from multiple monitors actively.

Other studies have shown that CCTV is often used by police to investigate crime (Ashby 2017; Dowling et al. 2019; La Vigne et al. 2011; Levesley and Martin 2005; Morgan and Coughlan 2018; Morgan and Dowling 2019). This is particularly true in areas with very high camera coverage, such as public transport networks. A recent study in Sydney, Australia, found that police requested camera footage from the operators of cameras monitoring the metropolitan rail network an average of 17 times per day. There is also growing evidence that access to footage helps police to solve crime. Ashby (2017) analyzed more than 250,000 crimes recorded on the British railway network over a 5-year period. He found that CCTV was available to investigators in almost half of all cases and was useful in two thirds of cases for which it was available. Moreover, when the CCTV was useful, the likelihood that law enforcement was able to solve these cases improved. Most recently, Morgan and Dowling (2019) showed that police access to CCTV footage, when investigating crimes on the rail network, improved the chances that an offender would be arrested, especially for property crime and late-night assaults. In a related study, footage was highly valued by investigators as it typically aided in their ability to identify or confirm the identity of a suspect (Dowling et al. 2019). Footage was most likely to be sought when other forms of evidence – specifically, witness statements – were not available (Morgan and Coughlan 2018).

Results tend not to be as positive in other locations, such as city centers, where the level of coverage is not as great. Kindgren and Marklund (2014) found that police sought access to CCTV footage for one in eight incidents that occurred in a two nighttime entertainment districts in Sweden, providing information relevant to the investigation in one in four cases. Likewise, King et al. (2008) examined the use of public space CCTV footage by detectives in San Francisco, finding that police only charged an offender in six of the 120 cases where footage was requested over a 3-year period.

In terms of the impact of video surveillance on physical security – whether in reducing crime, improving perceptions of safety, or helping police – results are mixed. But the research does show several factors influence whether CCTV is effective. Specifically, the type of crime being targeted, the level of coverage in public areas, the ability of cameras to capture entire incidents, the resolution and quality of images captured by CCTV, the amount and type of monitoring in place, the relationships between police and camera operators, and the presence of other security measures are improved through use of CCTV (Ashby 2017; La Vigne et al. 2011; Levesley and Martin 2005; Piza et al. 2019). Moreover, this information can be used to shape the ways in which video surveillance networks are designed, used, and managed.

Determining the Appropriateness of Video Surveillance

First and foremost, the evidence presented in this entry highlights the importance of careful

planning, starting with the decision as to whether video surveillance is the correct choice. Whether the goal is to prevent crime or to assist police investigate crime, CCTV should be installed in locations where there is a high concentration of criminal incidents. Additional consideration needs to be given to the types of offenses that occur in that location. The preventative benefits of CCTV appear limited mostly to property offending and possibly drug dealing and do not extend to preventing violent crime (Piza et al. 2019); however, police are more likely to seek access to CCTV footage for serious violent crime, while both property and violent crime investigations benefit from the availability of CCTV footage, albeit in different ways (Ashby 2017; Dowling et al. 2019; Morgan and Dowling 2019). Hence, CCTV is probably not the answer when the aim is to reduce (rather than investigate) a violent crime and disorder problem in city centers; but it may be the appropriate choice when the problem is crime in suburban areas or car parks. In any case, CCTV is most effective when used in combination with other intervention measures, including signage, lighting, security guards, and access control (Piza et al. 2019), which means it should be considered as part of a wider strategy to reduce crime.

Design Features of Video Surveillance Systems

Once it has been established that installing a video surveillance is an appropriate response, then the next step is to establish the requirements of the system, including technical specifications. This process includes details, such as the placement and positioning of CCTV cameras and the type of cameras that are used. Decisions will be influenced by the reasons for installing the system (and intended outcomes), as well as the specific characteristics of the location in which CCTV is to be installed.

A site audit will assist with respect to the layout of cameras to ensure adequate coverage. Camera coverage has been shown to have direct implications for the effectiveness of video surveillance both in preventing crime (Piza et al. 2019) and in enhancing criminal investigations (Ashby 2017; Morgan and Dowling 2019). However, the benefits appear limited to areas where it is possible for cameras to cover a large proportion of public space in a given area, whether that is a small location, like a car park, or bigger, but well-defined area, like an entire public transport network. Related to this issue is the placement of cameras – immovable obstructions to the line of sight of cameras not only impede the use of footage for investigations (Dowling et al. 2019), they are also associated with reduced prevention effects (Piza et al. 2014a). The presence of other forms of passive surveillance is also an important consideration because this will influence the availability of other evidence (i.e., witness statements; Morgan and Dowling 2019).

Image quality is obviously important, particularly with the use of video surveillance footage as evidence in criminal investigations. Studies have shown that when the quality of footage falls below a certain threshold, there can be a significant negative effect on the ability of operators to identify individuals captured on CCTV accurately. Keval and Sasse (2008) concluded that the optimal frame rate for detecting events and the analysis of events using video surveillance footage was eight frames per second, significantly lower than the industry standard for modern cameras. In selecting the appropriate equipment, it is useful to consider the range of requirements in terms of image quality, ranging from the need for sufficient resolution for crowd control through the ability to identify faces at a distance. The decision will be based on four factors: object to be observed, the level of detail, distance between object and camera, and lighting conditions. Compromises are, of course, necessary. Image quality is constrained by the quality of cameras and camera lenses (and equipment generally), the choice of which often depends on budget. But it can also be influenced by the level of video compression required to store images and the amount of storage available, which is, in turn, influenced by the length of time needed to store images (before they are recorded over). It is essential to ensure that decisions to maximize storage, for example, do not

come at the expense of image quality in such a way as to render the footage useless to investigators.

There is good evidence regarding the importance of ensuring that video surveillance systems are integrated with law enforcement responses (Alexandrie 2017; La Vigne et al. 2011; Piza et al. 2014a). Proactive enforcement of crimes detected on camera is a key factor in whether CCTV actually prevents crime, with the presence of active monitoring shown to increase the efficacy of video surveillance as a crime prevention measure based on dozens of studies (Piza et al. 2019). While the mere presence of CCTV may be sufficient to deter opportunistic offenders, the increased threat of arrest that comes from proactive enforcement may enhance this deterrent effect (Piza et al. 2014a). Footage must also be shared in a timely fashion post-incident; research suggests that the vast majority of footage requests are likely to be made within the first week following an incident (Morgan and Dowling 2019). Footage needs also be provided in a viewable format, since the inability to view images because of compatibility issues can hinder investigations (Dowling et al. 2019).

Of course, this result is conditional on an effective relationship between camera operators and law enforcement, but also may be attributed to the system design. In their large-scale observational study of control rooms, Gill et al. (2005) concluded that the design of control rooms had a significant bearing on how well they operated. Of particular note was the importance of camera-to-operator and camera-to-monitor ratios – the probability of detecting incidents declined substantially when the ratio of cameras to an operator exceeded 100. Likewise, a major contributor to the effectiveness of the surveillance network used on the train network in Sydney, Australia, was the ICT system that enabled rapid information sharing and communication between the security personnel working in the control room and the dedicated law enforcement officers and security staff able to respond to incidents (Morgan and Coughlan 2018). Integrated networks, such as where a video surveillance system is connected with the police radio network, allow for effective communication between camera operators and frontline responders (Gill et al. 2005).

However, effective implementation of video surveillance does not end at the design stage. Individuals and organizations that are responsible for procuring CCTV systems, distributers and installers, and camera operators each play an absolutely critical role in ensuring video surveillance is used effectively. The human element of video surveillance is an essential and sometimes overlooked consideration (Ratcliffe 2011). Research has tended to focus on the role of camera operators since actively monitored systems appear to be the most effective at preventing crime (Alexandrie 2017) and in extracting evidence for investigations.

There are different models in terms of who monitors CCTV footage, including police (which is rare, at least in some countries like Australia), security personnel, local government staff, and volunteers (Wilson 2005). Each model has advantages and disadvantages. In many jurisdictions, including in the United Kingdom and Australia, CCTV camera operators responsible for public space CCTV must possess a relevant security license, which mandates participation in accredited training for security personnel. The same is also true for installers of video surveillance systems. In the United Kingdom, operators must also obtain a frontline Public Space Surveillance license, which requires the completion of Security Industry Authority-accredited training. Training standards and packages specific to video surveillance exist in most countries, delivered by accredited training providers, but there are barriers to access, such as cost and awareness of availability (see ▶ "Physical Security: Methods and Practices" and ▶ "Security Guards: Academic and Training Programs" in this encyclopedia). Research has shown that operators often do not receive the training they require, and that factor negatively impacts the performance of video surveillance systems (Gill and Spriggs 2005).

Whether as part of mandatory licensing requirements or not, best practice dictates that camera operators should be provided with training in a range of areas, including training that

can enhance their performance as operators and technology or product-specific training (see ▶ "Physical Security: Best Practices" in this encyclopedia). Key areas for training, besides the obvious practical training on how to operate the system and camera equipment (and knowledge of CCTV generally), include effective monitoring practices, such as how to identify suspicious behavior, people, or objects, legislative and privacy obligations (which includes data storage and handling), effective communication, and the processes for storing and retrieving footage for investigative purposes. The importance of handling video footage appropriately so that it remains admissible in court as evidence cannot be overstated.

Managers are also vital, particularly in larger control rooms with multiple operators. Managers with technical expertise are able to liaise effectively with security contractors and operators and to share knowledge on system operation (Gill et al. 2005). Training for end users of footage may also prove beneficial. La Vigne et al. (2011) found support for training for prosecutors and defense attorneys in the use of video surveillance systems, system capabilities (and limitations), and presentation of footage when used in the courtroom.

Beyond training, it is also important that there be well-designed operational procedures for the effective monitoring of video surveillance, storage of camera footage, and sharing of footage for the purposes of criminal investigations. These protocols must align with relevant jurisdictional policies and legislation. They also make clear the responsibilities of camera operators and end users with respect to matters such as who is allowed to access to real-time and recorded footage, and in what circumstances, when this footage may be shared with third parties, and how to handle the disclosure of privacy breaches and processes for the effective management of video evidence. Certain procedures, such as those relating to video evidence, should be developed in close consultation with local law enforcement. Operational procedures should extend to protocols regarding the continuous length of time that operators spend monitoring footage, given the impact of mental fatigue on task performance (Faber et al. 2012), as well as the support provided to operators who witness traumatic or distressing footage to mitigate its harmful effects (Smith 2016).

A final important consideration with any video surveillance system is balancing the need for and potential benefits of surveillance with the need to respect the privacy of individuals. Privacy advocates and academics have long raised concerns about the impact of mass surveillance, particularly in circumstances in which video surveillance systems are connected with other technology, such as facial recognition systems.

While these issues are important, there are ways to protect the personal information collected via video surveillance systems. First and foremost, video surveillance systems must adhere to relevant planning and legislative guidelines. Each country has its own legislation, governing principles, or code of conduct for the use of CCTV, particularly as it relates to privacy. For example, the UK Government has released a Surveillance Camera Code of Practice (Home Office 2013), while in Australia the legislation varies between the states and territories and for different industries. Beyond these, there are general principles that help guide the ethical use of video surveillance for physical security. The European Forum for Urban Security (2010) has published a set of principles for video surveillance systems, designed to help ensure that the rights of citizens are appropriately protected. This includes ensuring that the use of video surveillance can be justified empirically, that the equipment is proportional to the problem it seeks to address, that the purpose and process for installing CCTV are transparent, that there is a process of accountability to the public, and that there is some degree of independent oversight. These provide useful guidance to those organizations planning on installing CCTV systems.

Conclusion

Video surveillance remains a popular physical security measure to serve the goal of preventing

crime or assisting police in response and investigation. Although there remains mixed evidence as to its crime prevention effects, there are clear benefits to law enforcement and security providers. When deployed strategically there is also good evidence that it can be effective in improving public safety and security. It is important, however, that video surveillance systems adhere to best practices with respect to their design, management, and operation.

Cross-References

- ▶ Physical Security: Best Practices
- ▶ Physical Security: Methods and Practices
- ▶ Security Guards: Academic and Training Programs

References

Alexandrie, G. (2017). Surveillance cameras and crime: A review of randomized and natural experiments. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 18*(2), 210–222. https://doi.org/10.1080/14043858.2017.1387410.

Armitage, R. (2002). *To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime*. London: Nacro Crime and Social Policy Section.

Ashby, M. P. J. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research, 23*(3), 441–459. https://doi.org/10.1007/s10610-017-9341-6.

BIS Research. (2018). *Global video surveillance market analysis and forecast, 2017–2023*. Retrieved from BIS Research website: https://bisresearch.com/industry-report/video-surveillance-market.html

British Security Industry Association. (2013). *The picture is not clear: How many CCTV surveillance cameras in the U.K.?* London: British Security Industry Association.

Dowling, C., Morgan, A., Gannoni, A., & Jorna, P. (2019). How do police use CCTV footage in criminal investigations? *Trends and Issues in Crime and Criminal Justice, 575*, 1–15.

European Forum for Urban Security. (2010). *The charter for a democratic use of video surveillance*. Paris: European Forum for Urban Security.

Faber, L. G., Maurits, N. M., & Lorist, M. M. (2012). Mental fatigue affects visual selective attention. *PLoS One, 7*(10), e48073. https://doi.org/10.1371/journal.pone.0048073.

Felson, R. B., & Massoglia, M. (2012). When is violence planned? *Journal of Interpersonal Violence, 27*(4), 753–774. https://doi.org/10.1177/0886260511423238.

Gerrard, G., & Thompson, R. (2011). Two million cameras in the U.K. *CCTV Image, 42*, 10–12.

Gill, M., & Spriggs, A. (2005). *Assessing the impact of CCTV* (No. 292; p. 176). London: Home Office.

Gill, M., Spriggs, A., Allen, J., Hemming, M., Jessiman, P., Kara, D., … Swain, D. (2005). *Control room operation: findings from control room observations* (Online Report No. 14/05). London: Home Office.

Grove, L., & Farrell, G. (2012). Once bitten, twice shy: Repeat victimization and its prevention. In D. P. Farrington & B. C. Welsh (Eds.), *The Oxford handbook of crime prevention* (pp. 404–422). Retrieved from https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195398823.001.0001/oxfordhb-9780195398823-e-20.

Home Office. (2013). *Surveillance camera code of practice*. London: Home Office.

Hulme, S., Morgan, A., & Brown, R. (2015). CCTV use by local government: Findings from a national survey. *Research in Practice, 40*, 1–9.

Johnson, S. D., Guerette, R. T., & Bowers, K. (2014). Crime displacement: What we know, what we don't know, and what it means for crime reduction. *Journal of Experimental Criminology, 10*(4), 549–571. https://doi.org/10.1007/s11292-014-9209-4.

Keval, H. U., & Sasse, M. A. (2008). To catch a thief – you need at least 8 frames per second: The impact of frame rates on user performance in a CCTV detection task. *ACM Multimedia*. https://doi.org/10.1145/1459359.1459527.

Kindgren, J., & Marklund, F. (2014). *CCTV surveillance of Stureplan and Medborgarplatsen*. Stockholm: Swedish National Council for Crime Prevention.

King, J., Mulligan, D., & Raphael, S. (2008). CITRIS report: The San Francisco community safety camera program. An evaluation of the effectiveness of San Francisco's community safety cameras. Berkeley, CA: Center for Information Technology Research in the Interest of Society, University of California.

La Vigne, N. G., Lowry, S. S., Markman, J. A., & Dwyer, A. M. (2011). *Evaluating the use of public surveillance cameras for crime control and prevention*. Washington, DC: U.S. Department of Justice.

Levesley, T., & Martin, A. (2005). *Police attitudes to and use of CCTV* (Online Report No. 09/05). London: Home Office.

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet, 10*(4), 415–453. https://doi.org/10.1002/poi3.183.

Lorenc, T., Petticrew, M., Whitehead, M., Neary, D., Clayton, S., Wright, K., … Renton, A. (2013). Environmental interventions to reduce fear of crime: Systematic review of effectiveness. *Systematic Reviews, 2*(1), 30. https://doi.org/10.1186/2046-4053-2-30.

McCahill, M., & Norris, C. (2002). *Estimating the extent, sophistication and legality of CCTV in London*. Hull: University of Hull, Centre for Criminology and Criminal Justice.

Mitchell, A., & Diamond, L. (2018, February 2). China's surveillance state should scare everyone. Retrieved 18 June 2019, From the Atlantic website: https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/

Morgan, A., & Coughlan, M. (2018). Police use of CCTV on the rail network. *Trends and Issues in Crime and Criminal Justice, 561*, 1–18.

Morgan, A., & Dowling, C. (2019). Does CCTV help police solve crime? *Trends and Issues in Crime and Criminal Justice, 576*, 1–16.

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2014a). Analyzing the influence of micro-level factors on CCTV camera effect. *Journal of Quantitative Criminology, 30*(2), 237–264. https://doi.org/10.1007/s10940-013-9202-5.

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2014b). Is the punishment more certain? An analysis of CCTV detections and enforcement. *Justice Quarterly, 31*(6), 1015–1043. https://doi.org/10.1080/07418825.2012.723034.

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy, 18*(1), 135–159. https://doi.org/10.1111/1745-9133.12419.

Ratcliffe, J. (2011). *Video surveillance of public places*. Washington, DC: U.S. Department of Justice.

Reaves, B. A. (2015). *Local police departments, 2013: Equipment and technology*. Washington, DC: U.S. Department of Justice.

Smith, G. (2016). Life through a lens: Risk, surveillance and subjectivity. *International Journal for Crime, Justice and Social Democracy, 5*(1), 82. https://doi.org/10.5204/ijcjsd.v5i1.281.

Space and Naval Warfare Systems Center Atlantic. (2013). *CCTV technology handbook* (p. 66). New York: U.S. Department of Homeland Security.

Wells, H., Allard, T., & Wilson, P. (2006). *Crime and CCTV in Australia: Understanding the relationship*. Gold Coast: Bond University.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly, 26*(4), 716–745. https://doi.org/10.1080/07418820802506206.

Welsh, B. C., Farrington, D. P., & Taheri, S. A. (2015). Effectiveness and social costs of public area surveillance for crime prevention. *Annual Review of Law and Social Science, 11*(1), 111–130. https://doi.org/10.1146/annurev-lawsocsci-120814-121649.

Williams, T. (2018, May 26). Can 30,000 cameras help solve Chicago's crime problem? *The New York Times*. Retrieved from https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html

Wilson, D. (2005). Behind the cameras: Monitoring and open-street CCTV surveillance in Australia. *Security Journal, 18*(1), 43–54. https://doi.org/10.1057/palgrave.sj.8340190.

Winge, S., & Knutsson, J. (2003). An evaluation of the CCTV scheme at Oslo central Railway Station. *Crime Prevention and Community Safety, 5*(3), 49–59. https://doi.org/10.1057/palgrave.cpcs.8140155.

Further Reading

Bowers, K. J., & Johnson, S. D. (2016). Situational crime prevention. In D. Weisburd, D. P. Farrington, & C. Gill (Eds.), *What works in crime prevention and rehabilitation* (pp. 111–135). New York: Springer.

Piza, E. L. (2018). The history, policy implications, and knowledge gaps of the CCTV literature: Insights for the development of body-worn video camera research. *International Criminal Justice Review*, 1–21. https://doi.org/10.1177/1057567718759583.

Taylor, E. (2018). CCTV: Reflections on its use, abuse and effectiveness. In M. Gill (Ed.), *The handbook of security* (pp. 705–726). London: Palgrave Macmillan.

Police: Public Versus Private Policing

Clarissa Meerts
Faculty of Law, Department of Criminal Justice and Criminology, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Keywords
Policing · Public versus private · Security · Investigations

Definition

Public and private initiatives to respond to disorder and crime.

Introduction

Policing is a very wide, and expanding, concept. While it naturally has a strong connection with "the police" as the entity for the execution of the monopoly over legitimate use of force by the state, policing as a concept goes much further than just the actions of the public police. For example,

policing may involve regulatory agencies (see, e.g., Mascini and Van Erp 2014), civilians (see, e.g., Van Steden 2009), and private security firms (see, e.g., South 1988). In this contribution, the concept of policing will be unpacked. In current society, "policing" can no longer be seen as the sole responsibility of any state actor, and so, both the public and the private side of policing are discussed.

High Versus Low Policing

Policing as a concept can be considered contested. First of all, there is a difference between high and low policing that is often not made in our day-to-day use of the concept. The origins of modern police are often placed with the efforts of Sir Robert Peel in the United Kingdom in the early nineteenth century. This type of policing is the "low policing," which we associate with the police organization. It consists, according to Brodeur (1983: 512), of "the forceful reaction to *conspicuous* signs of disorder" (emphasis in original). Low policing consists of the first line of defense against crime and disorder, by providing emergency assistance, reacting to signals from the public, controlling traffic, nightlife, and events, and by providing crowd control. "High policing," on the other hand, concerns itself with *political* policing. In the words of Brodeur (1983: 513), "it reaches out for potential threats in a systematic attempt to preserve the distribution of power in a given society." High policing is about gathering intelligence to ensure the stability and security of the state, rather than about security and safety of (parts of) the population (for a discussion of the difference between safety and security, see ► "Security: Concepts and Definitions"). This type of policing is usually not associated with the police but rather with national intelligence services.

Public Versus Private Policing

Going back in time, we can see that policing has a long history. Only in recent times have "policing" and "security provision" come to be seen as an exclusive task of the state (Garland 2001). Before the development of a modern, state-led police force, the provision of security was something that was a shared task of public and private entities. In most nation-states, an official police force has only been around for about 200 years (ibid.). With the professionalization of state policing, private forms of policing were increasingly diminished. However, even in these times, social control has never been merely state business. "Social control" may be defined as "the capacity of a society to regulate itself according to desired principles and values" (Sampson 1986: 277). This contains both formal (organized by the state) and informal (executed by private individuals and entities) forms of social control. While most of the *formal* policing might have been monopolized by the state in the last couple of centuries, *informal* policing (within families, companies, schools, etc.) remained present throughout history.

In more recent years, the involvement of private parties in policing has grown immensely (Button and Stiernstedt 2017). While the involvement of private parties in policing is by no means new, the development of a professional, commercial security market is (Shearing and Stenning 1983). Different perspectives are taken by different scholars as to the question of what caused such a development; however, most fall under one of two categories. On the one hand, there are those who focus on a "failure of the state argument" (also known as "fiscal constraint theories"). Because of restrictions in funding, state police organizations are unable to cope with the demand for security, arising from society (Jones and Newburn 1993). As a response, the state privatizes some of its functions to private parties, so as to release some of the pressure. Another strategy to solve the policing deficit is to "responsibilize" others to participate in policing. In this way, the state is able to avoid ceding its position to the private sector: while responsibility is shared, this is done under the banner (and on terms) of state policy.

In addition to these fiscal constraint theories, focusing on a receding state, there are those who see the growth of mass private property as the major force behind the expansion of private

policing (Shearing and Stenning 1981). In our current society, the line between public, private, and semipublic space gets blurred. Many daily activities now occur on (mass) private property, such as amusement parks and shopping malls. Both public and private policing occurs in these (semi)public and private spaces, and so power and responsibilities get fragmented and divided among public and private actors. Complex networks of policing combine to provide security within a society.

The difference between these perspectives is mainly the origin of the growth. Fiscal constraint perspectives lay emphasis on a gap that is created by a receding state and filled by private policing. Mass private property perspectives, on the other hand, state that there is a growing demand for security in (semi)private spaces, which logically leads to a growth in forms of private policing (Button 2004).

Another development that is important here is that of the shift toward "community policing." Although community policing as such is not new, it became very popular at the end of the twentieth century (Emsley 2007). Its popularity can be attributed to the existence of problematic police/community relations in many countries. Community policing is a very broad scope concept that can be used for many initiatives. It is often seen as more of a philosophy than a concrete program, which tries to focus on problem-solving within communities, with the use of partnerships (Cordner 2014). These public/private partnerships consist of police and other state actors and communities (e.g., neighborhoods) but also of different forms of private (commercial) policing.

Public and Private Policing Functions

While state-led policing can be divided into high and low policing, additional categories can also be identified. Within the policing task, there is, for example, a division between preventative (before the fact) and repressive tasks (after the fact). This distinction may also be made within private forms of policing. Before the fact private policing focuses on various aspects of security and safety, such as physical security (cash-in-transit, guarding of personnel or guarding of specific places such as an embassy, event, airport, the railway, maritime security, or a mall by security guards) or technical security services (such as alarm systems and camera surveillance and cyber security). After the fact private policing consists of private providers of corporate and investigative services, responding, for example, to instances of fraud or employee theft (for more on this, see ▶ "Investigations: Employee Theft of Employer Property").

The broad concept of "policing," being executed within both the public and the private sphere, often evokes heated debates on the question who should be responsible for policing. In criminology (and indeed, in Western society more generally), a tendency exists to place the emphasis on state efforts. As discussed above, many private forms of policing exist, and to expect the state to be the sole provider of security and policing services is not very realistic. Few scholars call for a situation in which policing is the sole responsibility of the state. However, the question does remain whether the state needs to be the primary actor in this or just one of the many policing localities (see ▶ "Security: Concepts and Definitions" for a brief discussion of this).

A point of principle in this debate is the argument that policing for profit by private security providers does not align with the common good focus of public police agencies (Loader 2000). Interestingly, recent research points in a direction that the division between public and private, in the sense that "the public police is working for the common good" and "private security is promoting private interests," paints a too black-and-white picture. In their 2018 article, Loader and White claim that security cannot be said to be a strictly "discrete commodity": private security guards are regularly confronted with situations in which private interest and public interest collide. One example of such a situstaion is one in which a security guard prevents a suicide attempt of someone while he is not hired to do so. Private interests and moral obligations are often weighed against each other, even within the commercial context of private policing. Meerts (2018) reports similar results when it comes to corporate investigators.

In the plural landscape of policing, drawing very clear distinctions is a complex endeavor.

Conclusion

The answer to the question of what "policing" actually is, is ever-changing. Policing can be seen with a narrow lens, merely consisting of the actions of the public police organization. This focus would then be on low policing by the state. However, over the past decades, the concept has been broadened to also include many activities by intelligence agencies (high policing efforts), regulatory agencies, and others. But not only is the concept of *what policing is* liable to change, so is the answer to the question *who executes* the policing activities. We now have a pluralized policing landscape, in which both public and private forms of policing are omnipresent. It remains a question for the future which direction policing is going to take – however it seems a safe bet that the concept will remain liable to change.

Cross-References

- ▶ Corporate Security
- ▶ Event Security
- ▶ Intelligence
- ▶ Investigations: Fraud
- ▶ Investigations: Employee Theft of Employer Property
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Public-Private Partnerships: Security Organizations
- ▶ Retail Security: Employee Theft
- ▶ Security: Concepts and Definitions

References

Brodeur, J.-P. (1983). High policing and low policing: Remarks about the policing of political activities. *Social Problems, 30*(5), 507–520.

Button, M. (2004). 'Softly, softly', private security and the policing of corporate space. In R. Hopkins Burke (Ed.), *Hard cop, soft cop: Dilemma's and debates in contemporary policing* (pp. 101–113). Cullompton: Willan Press.

Button, M., & Stiernstedt, P. (2017). The evolution of security industry regulation in the European Union. *International Journal of Comparative and Applied Criminal Justice, 41*(4), 245–257.

Cordner, G. (2014). Community policing. In M. D. Reisig & R. J. Kane (Eds.), *The Oxford handbook of police and policing* (pp. 148–172). New York: Oxford University Press.

Emsley, C. (2007). Community policing/policing and communities: Some historical perspectives. *Policing, 1*(2), 235–243.

Garland, D. (2001). *The culture of control; crime and social order in contemporary society.* Chicago: University Press.

Jones, T., & Newburn, T. (1993). *Private security and public policing*. Oxford: Oxford University Press.

Loader, I. (2000). Plural policing and democratic governance. *Social & Legal Studies, 9*, 323–345.

Loader, I., & White, A. (2018). Valour for money? Contested commodification in the market for security. *British Journal of Criminology 58*(6), 1–19.

Mascini, P., & van Erp, J. (2014). Regulatory governance: Experimenting with new roles and 635 instruments. *Recht der werkelijkheid, 35*(3), 3–11.

Meerts, C. A. (2018). *The semi-autonomous world of corporate investigators. Modus vivendi, legality and control*. Rotterdam: Erasmus universiteit Rotterdam.

Sampson, R. J. (1986). Crime in cities: The effects of formal and informal social control. *Crime and Justice: A Review of Research, 8*, 271–311.

Shearing, C. D., & Stenning, P. C. (1981). Modern private security: Its growth and implications. *Crime and Justice, 3*, 193–245.

Shearing, C., & Stenning, P. (1983). Private security: Implications for social control. *Social Problems, 30*(5), 493–506.

South, N. (1988). *Policing for profit: The private security sector*. London: Sage.

van Steden, R. (2009). Burgerparticipatie in lokale veiligheidsnetwerken: over 'nodale sturing' en 'verankerd pluralisme'. *Justitiële Verkenningen, 35*(1), 29–42.

Further Reading

Button, M. (2002). *Private policing*. Cullompton: Willan Publishing.

Johnston, L. (1992). *The rebirth of private policing*. London: Routledge.

van Steden, R. (2007). *Privatizing policing: describing and explaining the growth of private security.* Den Haag: Boom Juridische uitgevers.

Walby, K., & Lippert, R. (Eds.). (2014). *Corporate security in the 21st century: Theory and practice in international perspective*. Basingstoke: Palgrave Macmillan.
Wood, J., & Shearing, C. (2007). *Imagining security*. Cullompton: Willan Publishing.

Private Detectives

Susan Pickman
John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Custody investigation · Fraud investigation · Marital investigation · Private investigation services · Professional investigators · Surveillance

Definition

A private detective also termed "private investigator" (PI) is a person who is a fact finder or evidence gatherer and is hired directly by businesses (e.g., law firms, corporations, insurance companies) or individuals to gather intelligence and confirm or disprove information.

Introduction

PIs are, at the most basic level, information-gatherers. Their job is to find information about persons, places, and things on behalf of clients. Finding the information can involve a wide range of activities, from interviewing people in broad daylight, to conducting undercover surveillance late at night. Most of the time, however, the primary business of a PI involves knowing where to look or whom to contact for information. And while today, quite a lot can be found online, the stock and trade of a private investigator is the ability to reach out – personally – to someone who will have the information they need.

Because the job of a PI so often involves obtaining information from others, the essential quality of a successful PI is the ability to relate to other people. They also should possess a broad knowledge of human behavior and have an inquisitive mind. Given that these traits can be picked up in a variety of settings, private investigators come from all walks of life.

At one time, it was uncommon for anyone but a former police officer to be a private investigator. Now, however, attorneys will sometimes move into investigative work, or a PI may come from an entirely different field such as psychology. In fact, private investigators can have almost any sort of educational background, with the most common degrees being in security management, criminal justice, psychology, or even history. Nevertheless, the best investigators have some education specifically in investigations. Some colleges offer credit courses and training in criminal and private investigations, and it is best for a PI to have exposure to both. However, a lack of formal training can be supplemented with – and enhanced by – field experience working with a detective agency or law enforcement or as a paralegal or news reporter.

In most states, to solicit business and practice, a private investigator/detective must have a state license. The most current state requirements can be accessed through the website of IASIR (The International Association of Security and Investigative Regulators) www.iasir.org. Because licensing is conducted on a state-by-state basis, licensing requirements vary. However, most states require PIs to be at least 25 years old, have a high school diploma (or the equivalent), have US citizenship or residency, and pass a test. States might also mandate up to 3 years' experience working in law enforcement, investigations, or another full-time job. Most states also require a private investigator to get a bond, which protects the state from being liable for improperly issuing a license.

Finally, it is essential for a PI to have a clean record. Some states will refuse to issue a PI license to candidates who have a felony or misdemeanor conviction. Clients will also often look for other indicators of responsibility and reliability. A potential client conduct a Google Search, but they may also wish to verify that the investigator does indeed

possess a PI license, to see evidence of any professional memberships. Work history also points to whether the PI is responsible and reliable. Many of the best PIs do not advertise at all.

Clientele and Ethics

Private investigators work for attorneys, corporations, courts, and individuals. They are hired by companies to research personnel, such as pre-employment investigations; they may also be asked to help conduct due diligence for business acquisitions or mergers. However, PIs are most often hired by attorneys because they possess complementary expertise that the attorney needs to bring a successful conclusion to a case. Attorneys often need information to determine whether an accused person has a reliable alibi, finding a witness or they need hard-to-obtain details to reconstruct an accident. The PI is then hired to obtain this information.

Private investigators accept cases based on a variety of factors. The most well-regarded PIs turn down more cases than they take, sometimes because the scope of the work is not within their expertise, but more often because prospective clients are not willing to pay what the PI deems their time and services are worth. Personal values and legal ethics also influence what work a PI is willing to take. Some individuals may approach a PI to help them break the law – to conduct inappropriate surveillance in order to circumvent a restraining order, for example. Even attorneys are not always ethical; for instance, an attorney might ask a PI to pose as a law enforcement officer to obtain information or to sign an affidavit that the attorney, not the PI, has prepared. In effect, investigators should be as discerning as their clients when choosing who to work for, and just because they can find information does not necessarily mean that they should.

Cooperation with Law Enforcement

Private detectives can cooperate with law enforcement officials. In some instances, these partnerships are official and long-lasting. The PI will initially investigate a case and then turn it over to law enforcement. In one example of such a situation involving trust funds, one trustee claimed to have lost some money in a bad business deal, but other stakeholders suspected that the money had been stolen. These stakeholders approached a law firm, who then hired a PI (who specialized in fraud) to work through stories of how the business deal went bad. Ultimately, the PI uncovered multiple phony corporations and determined that the trustee had lied and had stolen the money. The attorneys then took the case to law enforcement.

Specializing

Becoming a truly top-notch detective – and in turn being able to command the highest hourly rate – requires expertise, or specializing, in a particular area. According to a survey by PInow.com, some of the most common specialties are background checks, civil investigations (gathering evidence for a civil trial), surveillance, and fraud (Faber 2013). By specializing, a PI can solicit a specific type of client, or they can transition into related fields (e.g., polygraph examiners or cybercrime investigators).

Training to become an expert can be done in a variety of ways. For instance, before striking out on their own, a PI may take training courses while working in law enforcement, serving in the military or working for a private investigations firm with a particular specialty. Organizations (e.g., American Society for Industrial Security [ASIS], Association of Certified Fraud Examiners [ACFE]) offer certifications in investigations and fraud examination. Other organizations offer qualifications in arson investigations and accident reconstruction. These associations train individuals in a given specialty and then typically require testing, years of field experience, and at least a bachelor's degree to become certified.

Expert Witness

To become known as an "expert" in a given area, a PI needs extensive experience, a reputation as a

knowledgeable specialist, training, and credibility earned through the accolades of other professionals working in that area. To be deemed an "expert," a judge accepts the PIs' credentials and allows the PIs' testimony in a trial. When this happens, it means that the court has considered the PI to have the knowledge and expertise necessary to satisfy a judge in a particular case. Sometimes, the judge requires an investigation to be done to determine if a theft has occurred and if so, who is responsible. For example, a guardianship case might require an investigation to determine if a guardian is stealing from an elderly client. The court "hires" the investigator and pays them for their services. An expert PI may also work directly for an attorney, either prosecution or defense, as a "testifying expert." In this case, the PI is paid to take the stand in court and answer very pointed questions – some of which may attack the investigator's credibility. Not every PI finds this type of work desirable, but it is one way to charge a higher rate for having acquired a certain level of expertise.

PIs can take on the role of a consultant, charging an hourly rate to read over all of the documents in a case. If they disagree with the basic premise of the argument, they will be paid for identifying holes in the case by an agreement, but they need not continue to testify for that attorney and their client. This might happen where an individual has been accused of committing a crime. As an expert witness, the PI may be called upon by the attorney to say that the evidence indicated that the defendant is not guilty. However, after reading all of the materials, the PI believes that the individual is guilty, in which case it would not be appropriate for the expert to testify for the defense.

Why Hire a Private Detective?

The role of the private detective has become more complicated in the last two decades. The legal needs of private citizens and the corporate world have expanded, public law enforcement's numbers have not kept up, and as a result, the responsibilities of each civil servant working within the police force have broadened. Law enforcement has increasingly turned its attention – and has allocated its resources – to violent crime and counterterrorism (The Department of Justice, Office of Public Affairs 2011). This shift in attention has left lesser criminal, civil, and administrative investigatory responsibilities neglected, and as such, private citizens and corporations who are unwilling to wait for law enforcement to "get around" to investigating their issue have turned to private detectives.

Besides impatience with public law enforcement, another reason private citizens may be inclined to hire a private detective is that of his or her ability to handle the overlap in "type" of an investigation. For instance, a PI could be working on a case of corporate insurance fraud and discover that there is a criminal conspiracy that goes well beyond the insurance claim that the company initially hired the detective to investigate. Similarly, a missing person's case might turn into something very different if the private investigator discovers that the individual has been murdered.

Missing person's cases are the perfect example of work that is ideal for a PI rather than a civil servant detective. Law enforcement will not look for a missing adult unless there is some evidence of foul play or diminished capacity; however, PIs – if they accept the case – will look for a missing person under virtually any circumstances. Therefore, a family or attorney might hire a private investigator to locate a person because they wish to settle an estate, or an adopted child (now an adult) may want to find their biological parents – cases that a detective working for law enforcement would never take.

Casework Examples

Many private investigators say that their reason for being in the business is the unexpected nature of the casework they get to pursue. Their work is limited only by the legality of what the client wishes to pursue, the client's budget, and the skills and experience of the investigator.

The following real-life cases illustrate the depth and breadth of work an investigator may undertake. All of these cases have been made

public through court documents; in no instance did a private investigator violate his or her oath of confidentiality by sharing details of the case. However, some names have been changed to maintain privacy.

Case 1: Mary James, Sole Residence
Susan Pickman, NYS Licensed Private Investigator, and Certified Fraud Examiner

In most investigative cases, the key is to know which research tools to use and to persist in using them until some lead takes the investigator to the data required. This is how Susan Pickman, a New York State licensed private investigator and former police officer, pursued and solved the primary residence case of Mrs. Mary James.

Mrs. James was a senior woman who received subsidized housing in Europe. The landlord, John Jones, claimed that she was living elsewhere, which violated her legal requirement to live in the apartment as her sole residence. Mr. Jones wanted to revoke Mrs. James right to the property, but first, he needed to prove that Mrs. James was living in another country. He required an NYS licensed private investigator, which is how he hired Susan Pickman.

Pickman began her search for evidence of Mrs. James' residence elsewhere by looking through a number of public and proprietary databases. She found no trace of the woman, but she did discover an address for her son. By visiting this residence, Pickman found Mrs. James living there, and her affidavit was enough to allow European courts to issue a finding in favor of Mr. Jones.

Private investigators must often look tenaciously and use inconvenient or unconventional means to find the answers they seek. Thus, a great PI must have a voracious appetite for research and a keen ability to make links between seemingly unrelated information.

Case 2: Jack Patch, Missing Person
Charles-Eric Gordon, Esq., Investigative Counsel

While private investigators tend to specialize, most take at least one missing person's case. Such is the case of Jack Patch. This case was pursued by Charles-Eric Gordon, a New York State licensed attorney who conducted investigations into matters with a legal connection. (Due to being a licensed attorney, he was exempt from needing a private investigator license [Application of Article, NY GBS § 83].)

In 1988, Gordon was hired to investigate the disappearance of Jack Patch, the husband of Sarah Patch, who had recently died. Sarah and Jack had separated before Sarah's death, but Sarah set up a testamentary trust that would pay a generous amount of money each year to Jack, as long as he never divorced her and never married anyone else.

Checks from the trust had been delivered to a PO box in Manhattan – and cashed – for years until, in 1986, the PO box was suddenly closed with no forwarding address. The estate manager needed to either find Jack or confirm his death and locate next of kin, and so he hired Gordon.

Gordon began his investigation by consulting the white page directories and calling every listing with the name Patch. Eventually, he connected with Jack's brother Joseph, who shared that Jack had been born in 1898 and was buried somewhere on Staten Island. Because Gordon knew that Sarah, Jack, and their families were Jewish, he called Jewish cemeteries until he located Jack's grave.

As he awaited Jack's death certificate, Gordon continued to seek out Jack's next of kin. The cemetery records had listed a second wife, Ida, but when Gordon tried to locate her, he was unsuccessful. Instead, he found and spoke with Jack's nephew David, who implied that Jack and Ida had been married before Sarah died. To confirm this, Gordon once again used telephone directories to hunt down Jack's daughter Randy. Randy ultimately confirmed that her mother (Ida) and father (Jack) had had a bigamous relationship, which defrauded the trust since bigamy was and still is a felony in New York.

What makes Gordon's investigation particularly interesting is that it occurred in 1988 and 1989, before the Internet and online proprietary databases. Consequently, it involved a lot of telephone work and writing away for public records. This legwork is important to note, because while a lot of data is accessible by computer today, it would be misleading to assume that this cuts down on the amount of research involved in a PI's job. In fact, a lot of online data is wrong and must, therefore, be carefully double-checked for accuracy and to ensure that no "red herrings" lead the investigator astray.

Case 3: Bob's Carpets, Arson
Bruce H. Hulme, Certified Fraud Examiner and Board Accredited Investigator

This case was about whether the owner of Bob's Carpets, a carpet factory in Dalton, GA, had hired an arsonist to burn it down so that the owner could collect from the insurance company. The insurance company had determined that the fire had been set intentionally, but the owner's alibi was airtight, so the insurance company hired Bruce H. Hulme, a certified fraud examiner and board accredited investigator, to identify the arsonist and ascertain if the owner had hired him or her.

When Hulme eventually located the professional arsonist in New Jersey, arrangements were made for his arrest by the Georgia Bureau of Investigation, and he was given immunity to testify against Bob, who he stated had hired him. However, the trial was to take place in the US district court for the Northern District of Georgia in Rome, and the law firm representing Bob was a "The Northern Georgia law firm representing Bob (a "Good Ole Boy")," whereas the insurance company, based in New York, had hired a "Yankee" firm. Consequently, the insurance firm lost the case, in spite of Hulme's having identified the arsonist and acquired his confession.

The lesson from this case is that investigative work – even successful investigative work that uncovers the evidence a plaintiff or defendant needed – does not always result in the legal case being won. Hulme was hired to investigate an arson case, and while he successfully verified that arson had, in fact, been committed and identified the perpetrator, his side still did not win the court case.

Conclusion

Private detectives are needed now more than ever before. Whether they work with law enforcement, legal counsel, corporations, or private individuals, the job of a PI is to persevere in finding information that others do not have the means, skills, or time to unearth. The work can be both tedious and challenging and requires both a voracious appetite for detail and the ability to engage and observe others. While PIs can come from a variety of professional and educational backgrounds, almost all will need field experience and a state license to work as a professional private detective. Once they obtain a license, PIs can continue with formal training and solicit particular work to specialize in an area like fraud, arson, or civil investigations. Specializing can then lead to cooperation with certain types of law enforcement or attorneys and can also result in being called as an expert witness in civil and criminal trials. Finally, no matter the client, a PI should always exercise discretion in deciding whether or not to take a case; just because they can find something or someone does not always mean that they should.

References

Application of Article, New York General Business Law GBS § 83.

Faber, K. (2013). The 10 most common specialties of private investigators. PInow.com. Retrieved from https://www.pinow.com/articles/1737/the-10-most-common-specialties-of-private-investigators

The Department of Justice, Office of Public Affairs. (2011, September 7). *Fact Sheet: The Department of Justice ten years after 9/11* [Press release]. Retrieved from

https://www.justice.gov/opa/pr/fact-sheet-department-justice-ten-years-after-911

Further Reading

Becnel, P. (2017). *Introduction to conducting private investigations: Private investigator entry level (02E)*. Dublin: Coventry Publishing House.

Nemeth, C. P. (2010). *Private security and the investigative process* (3rd ed.). Boca Raton: Auerbach Publications.

Protection and Security in Public Spaces

Spyridon Triantafyllou
John Jay College of Criminal Justice, New York, NY, USA

Keywords
Protection · Public spaces · Security · Safety · Openness

Definition

Measures to suggest, establish, and implement for public safety in non-private locations.

Introduction

Public safety is highly prioritized in political agendas because the sentiment of security affects public opinion. Especially after the 9/11 terrorist attack, much emphasis has been placed by public authorities on recommending, planning, and implementing security and safety countermeasures in order to protect the public.

Research has shown that, over the last two decades, private interests and security in public spaces have changed public spaces to regulated places of consumption (Low and Smith 2006). Public social life increasingly falls within privately controlled spaces policed by security officers operating not in the public interest, but in the interests of their employers or corporate clients. Security in public spaces is thus connected with formal social control, projected mainly by manned security, such as security guards and other personnel and security devices, such as CCTV (Iveson 2007).

Defining Public Spaces

In order to define the term "public," the traditional dichotomy cleavage "public – private" is useful in the context of this analysis. *Public spaces* are places where individuals can claim full rights of access, use, action, and appropriation (De Backer et al. 2016). However, public spaces (e.g., shopping malls, park benches, and public streets) can be fully or partially controlled by limiting the extent of the openness of these spaces (i.e., *quasi-public spaces*, such as malls or other downtown areas) (Altman and Zube 1989; Jackson and Valentine 2016).

The origin and role of control is also connected with the notions of ownership and openness in relation to the "public–private" dichotomy. According to Wakefield (2003), there are four types of spaces based on this dichotomy: open public spaces; restricted public spaces; open private spaces; and restricted private spaces.

Open public spaces are spaces that are publicly owned and freely accessible. However, whether a member of the public may claim a legal right to enter such spaces depends on the type of space. Such a right exists in relation to access to public highways, and to open spaces, such as parks and recreation grounds, when public rights of way are set out in the statutory provision for those spaces (Wakefield 2003).

Restricted public spaces are publicly owned and access is only offered to those who fulfill certain admission criteria. These places may include publicly owned facilities at which an entry fee is charged, such as a leisure center owned by a local authority. Since a fee is required to restrict access, those who pay the fees can

access the space. Moreover, the restrictiveness of access depends on the space. For example, hospitals and military establishments have restrictive criteria for access (Wakefield 2003).

Open private spaces are privately owned territories, where free access by any visitor may be seen as implicit since visitor may claim no legal right of access to the premises unless it contains restriction of way. It is common to differentiate *public spaces* in general from *open private spaces* that are used for commercial purposes (i.e., shopping centers, leisure parks, passenger airports owned by private companies, and some business parks) (Wakefield 2003).

Restricted private spaces include private residencies or dwellings and privately controlled recreational areas where entry fees are charged (i.e., cinemas or football clubs) and/or membership is required (i.e., health or social clubs) (Wakefield 2003).

Analyzing Security as Element of Protection

For purposes of analysis and discussion, the concepts of "security" and "(life) safety" are to be taken into consideration. Although these terms are distinctly approached, they are closely interwoven and interdependent, and oftentimes they appear to be the same thing. In doing so, the notions of "security" and "safety" might provide useful insights about the concept of "protection" as a whole in public domain. Security is mostly related with crimes, while safety is mostly related with fires and accidents.

> [S]ecurity (derived from the Latin word *securus*) means "the state of being secure; freedom from danger or loss" (McCrie 2007) and has numerous definitions implying a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of such disturbance or injury. Safety, or life safety, or fire life safety, (derived from the Latin word *salvus*) means "the state of being secure; freedom from danger" (McCrie 2007) and has similarly numerous definitions which involve minimizing the possible danger to life and property from various threats. (Craighead 2009)

Security refers to protection and involves enforcement and suppression, while *life safety* refers to care and involves medical care and emergency response. But, in general, despite that these concepts are not well conceived in colloquialism, people usually are able to connote security with law enforcement agencies (i.e., police departments), safety with emergency services (i.e., fire departments), and, therefore, they are able to assume protection in total which includes both security and life safety.

Focusing on public spaces, the distinction between "security" and "safety" is of paramount importance. It is critical because not only does it enable us to know if an emergency arises, which is its nature and who is responsible for that (i.e., a police department or a fire department), but it also helps us to mitigate risks deriving from several situations by assessing the relevant threats.

From a security perspective, there may be threats such as crimes, active-shooting situations, suicide-bombings, cyberterrorism, or CBRN attacks, while from a safety perspective, there may be threats such as fires, natural disasters, traffic accidents, or communicable diseases. A threat is any indication, circumstance, or event with the potential to cause loss of or damage to an asset (FEMA 2005). Threats may be intentional, accidental, or natural disasters, while some of these threats may be considered asymmetric in nature.

The boundaries that characterize the private and public spheres are blurred in a risk society because of directives from institutional and state levels that often emphasize personal responsibility. However, public spaces become an even greater source of insecurity in a risk society (Van Brunschot and Kennedy 2008). An important tool for determining the "security" and "life safety" needs of an asset is risk management. Therefore, the distinction of security and safety is valuable for methodological purposes in terms of identifying vulnerabilities of assets, especially if these

assets are publicly accessible or located in a public space.

According to the law and standards in place, it should be obvious who is the authority having jurisdiction when a security or a safety issue occurs. Also, it should be clear who are the competent police or fire departments to operate in a public space which allows the agencies to perform in a superior manner, both in operational and strategic level.

Methods for the Protection of Public Spaces

This section aims to provide a generic methodology including all four spaces as mentioned above, rather than focusing on one specific type of public space. The methods suggested are supposed to be practical and help readers understand how public spaces are protected and secured.

According to Garcia (2006), when designing (or changing or updating) the physical protection system of a public space, the information gathered by a security management expert should include: the (a) physical conditions; (b) facility operations; (c) facility policies and procedures; (d) regulatory requirements; (e) legal issues; (f) safety considerations; and (g) the goals and objectives of each organization tasked with the protection of the public space.

First of all, it is imperative to request information about the physical conditions and physical infrastructure of facilities. The information provided to the security expert or other person or agency responsible for protection of public spaces should include: the site boundaries; the complexity of facility, areas, and other sub-areas; room locations within the facility; access points; existing physical protection features (if any); and all infrastructure details, such as heating, ventilation, and air conditioning system (HVAC) system, communication paths, construction materials of walls and ceilings, locations of any hazardous materials, and exterior areas. Information about the existing physical protection system, including (but not limited to) fences, sensors, cameras (CCTV), entry control systems, barriers, response force availability, should also be provided (Garcia 2006). Finally, it is crucial for security professionals to be apprised of whether the facility utilizes a contract or proprietary security force (if any) and its capabilities (Garcia 2006).

Second, the security expert should be aware of facility operations, including daily operations, employees, units, and divisions without the organization and operating conditions (working hours, off-hours, emergency operations), as well as the types and numbers of employees involved or affected by security operations. The existence or implementation of a security system may affect or restrict the work of the facility. Moreover, the supporting functions are to be evaluated, including procurement procedures, computing resources and distribution, maintenance activities, asset tracking, operational involvement and location of senior executives, workflow, shift changes, employee benefits, shipping and receiving, accounting functions, and any other supporting functions. Finally, information regarding the transition periods at the facility, especially during the shift change, if applicable, and the vehicle activity into and out of the facility, should be obtained (Garcia 2006).

Third, the security expert must know and understand all written and unwritten policies and procedures throughout the facility. In doing so, the expert can identify whether the occupants follow such policies revealing any lapses in order to update or modify these policies to mitigate risks and reduce liability. In any case, security managers must agree not to divulge any information, classified or not, related to the facility. In addition, corporate policies should exist documenting that all occupants, such as employees, residents, customers or visitors, respect additional rules about budgetary issues, privacy, using drugs or alcohol, and other expectations. To this end, whether there is a pertinent training program or not, and further whether its results meet the minimum expectations of security or not, should be documented. It is crucial to reinforce and promote a sentiment of "security culture," particularly in a diverse and crowded urban environment. It is crucial to create, establish, and preserve a culture of security, especially with so many and different tenants within a so complicated environment of the metropolitan area (Garcia 2006).

Furthermore, the socioeconomic and political environment, regulatory requirements and legal issues are to be considered when protecting public spaces. The security expert must be in a position to critically think about what policies and laws are applicable for all tenant organizations and the facility as a whole, either as a mandate or in order to increase security. Also, the knowledge of previous history regarding privacy, labor relations, training of guards and tenants, criminal statistics, and other legal issues are critical to reduce liability as a result of an overreaction or failure to protect. This corpus of knowledge must not be outside of safety considerations. Security experts must meet and collaborate with facility managers or other persons who are responsible for safety. Although security and safety may have different goals, they are considered complimentary functions. The term "integrated solutions" is used to project this desire and culture for coexistence of security and safety issues (Garcia 2006).

Finally, whether an employee of the facility or not, the security expert must partner in the strategic plan of senior management of all organizations residing in the high-rise building. Respecting their policies and issues of privacy, the security manager must know the potential threats, assets, and vulnerabilities of each and every occupant organization. Also, if necessary, mutual aid agreements with other organizations or industries should be at expert's discretion after consultation with C-suite level of management. That said, a security manager must be extrovert and develop relations with other facilities and identify who is the liaison between the facility and local law enforcement (Garcia 2006).

Focusing on "physical security," the following goals for security countermeasures are suggested for public places. There are three main goals for all security countermeasures (Norman 2015): (a) where possible, identify and deny access to potential threat actors; (b) deny access to weapons, explosives, and dangerous chemicals to the facility (except for legitimate exceptions, which should be well controlled and monitored); and (c) make the environment suitable for appropriate behavior, unsuitable for inappropriate or criminal or terroristic behavior, and mitigate the actions of both hazards and threats.

> [P]ractically, these goals are achievable mainly through specific functions, which are: "access control"; "deterrence"; "detection"; "assessment"; "response (including delay)"; and "evidence gathering", among others. Of particular importance are detection of an adversary, delay of that adversary, and response by security personnel, using hi-tech, lo-tech, and no-tech countermeasures. (Norman 2015)

Prior to designing a physical protection system, it is crucial to set the objectives, or simply state what to protect and against whom. Moreover, beginning with the designing of the system, the integration of people, procedures, and equipment is necessary in order to meet these objectives. At the same time, designing should consider issues regarding safety, as well regulatory, operational, legal, and economic limitations (Garcia 2006).

Furthermore, information should be obtained about the type of facility to be protected, which in turn will show the level of protection needed based on the percentage of publicly owned space. For instance, the security management professional should clarify whether a facility is public, or part of the facility is public, though privately owned. In doing so, one may understand potential private ownership constraints, which in turn may affect the overall security operations and performance. Second, identifying and defining threats for the facility is of the utmost importance, a process which needs effort and time. A threat definition is a detailed description of the physical threat by a malevolent adversary to the system. In addition to that, the concept of design basis threat (DBT) of the facility should be established in order to facilitate decision-making and establish technical requirements for security of the facility (Garcia 2006). For public spaces, certain threats, such as crimes or active-shooting situations, may harm public safety and impact on social and economic life. Finally, it is of the utmost importance to consider all as discussed above, in order to adopt risk mitigation strategies by improving the capacity to manage organizational risk of facilities in public spaces.

Public spaces that are considered "soft targets" for crime and terrorism require special consideration. *Soft targets* include locations difficult to

defend or usually undefended, typically non-governmental sites – and oftentimes places where people congregate in large numbers – as well as targets of some other value (e.g., national monuments, hospitals, schools, sporting arenas) (Robbins 2006). Typical acts of terrorism perpetrated against soft targets are attacks to public transportation, such as the 2004 series of coordinated explosions on commuter trains in Madrid, which killed 191 and wounded over 2000, and the July 2005 terrorist attacks in London, whereby four perpetrators carried out coordinated suicide bombings on a bus and three subway cars in London, killing 52 people (Law 2009). These and other public spaces are particularly challenging to secure. Nevertheless, soft targets may be "hardened" by adding layers of defense. Defensive measures aim to deter and with respect to public spaces are the following: barriers; surveillance' checkpoints; ID protocols; establishing of choke points for people or traffic flow; and restricting vehicle access to buildings or areas near them (Robbins 2006). The use of technology (e.g., CCTV) in such public areas contributes to creating a sense of security in all occupants (employees, residents, customers, or visitors) (Wakefield 2003).

Additional Practical Considerations for Establishing Public Safety

Security management experts may face security, safety, or both types of challenges, when evaluating or installing relevant devices in non-private facilities or assets, either open or not. Consequently, they should have in-depth knowledge of the functions of security and safety. In fact, a security expert or a security-oriented organization (either public or private) is called to identify and deal with any potential threats that are either security-driven or safety-driven threats.

It is expected that the security management expert is (or the team of experts are) knowledgeable of state-of-the-art security and/or (fire) (life) safety systems that are in compliance with policies and laws, as well as experienced in conducting security and/or safety surveys, particularly in public spaces. For instance, security countermeasures for accessibility should be in compliance with Americans with Disabilities Act (ADA), which is applicable to businesses and other organizations that operate places of public accommodation (i.e., restaurants, theaters, transportation facilities, retail stores, doctors' and lawyers' offices, private schools, day care centers, libraries, and hospitality facilities) (Atlas 2013). Moreover, the experts may have certain professional qualifications that would qualify them to be called to make or implement recommendations or in the event of future litigation to testify on behalf of the building owner or operator (Craighead 2009). Last but not least, such experts should have a well-established professional relationship with local law enforcement or fire authorities having jurisdiction.

A security formula is recommended for protection management experts that incorporates the a "Crime Prevention Through Environmental Design" (CPTED) concept into security ordinances, resolutions, and guidelines. "[A]ccording to the Defensible Space Theory, CPTED takes advantage of the practical considerations of "territoriality", which essentially means to reassign the physical areas of a space, which in turn will enhance local people to better control the environment and in particular public spaces. . .Territoriality can be accomplished by using a hierarchy of space as defined in Defensible Space Theory, such as subdividing public spaces into semi-public and semi-private places" (Atlas 2013). Elaborating on the "Crime Prevention Through Environmental Design" (CPTED) concept, a design is proper if it recognizes the designated use of the space; defines the crime problem incidental to and the solution compatible with the designated use; and incorporates the appropriate crime prevention strategy that enhances the effective use of space (Atlas 2013).

Conclusion

Security is becoming a greater priority in the design, construction, operations, and management of buildings and facilities.

Cross-References

- ▶ Educational Institution Safety and Security
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Interior Applications
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Rail (Train) Security

References

Atlas, R. (2013). *21st century security and CPTED: Designing for critical infrastructure protection and crime prevention*. Boca Raton: CRC Press.

Craighead, G. (2009). *High-rise security and fire life safety* (3rd ed.). Burlington: Butterworth-Heinemann.

De Backer, M., Melgaço, L., Varna, G., & Menichelli, F. (2016). *Order and conflict in public space*. New York: Routledge.

Federal Emergency Management Agency (FEMA). (2005). Risk Assessment A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings. Available at: https://www.fema.gov/media-library-data/20130726-1524-20490-7497/fema452_cov_toc.pdf.

Garcia, M.-L. (2006). *Physical protection systems* (2nd ed.). Burlington: Butterworth-Heinemann.

Iveson, K. (2007). *Publics and the city*. Oxford: Blackwell.

Jackson, L., & Valentine, G. (2016). Rethinking spaces, sites and encounters of conflict in twenty-first century Britain: The case of abortion protest in public space. In M. De Backer, L. Melgaço, G. Varna, & F. Menichelli (Eds.), *Order and conflict in public space*. New York: Routledge.

Law, R. (2009). *Terrorism a history*. Malden: Polity Press.

Low, S., & Smith, N. (2006). *The politics of public space*. New York: Routledge.

McCrie, R. (2007). *Security operations management* (2nd ed.). Burlington: Butterworth-Heinemann.

Norman, T. (2015). *Risk analysis and security countermeasure selection* (2nd ed.). Boca Raton: CRC Press.

Robbins, S. (2006). Soft targets, hard choices. In J. Forest (Ed.), *Homeland security: Protecting America's targets, volume II: Public spaces and social institutions*. Westport: Praeger Security International.

Van Brunschot, E., & Kennedy, L. (2008). *Risk balance and security*. Thousand Oaks: Sage Publications.

Wakefield, A. (2003). *Selling security: The private policing of public space*. New York: Routledge.

Further Reading

Alasdair, J. (2014). *On south bank: The production of public space*. Burlington: Ashgate.

Altman, I., & Zube, E. (1989). *Public places and spaces*. New York: Plenum Press.

Ball, D., & Ball - King, L. (2013). Safety management and public spaces: Restoring balance. *Risk Analysis, 33*(5), 763–771.

European Conference of Ministers of Transport (ECMT). (2003). *Vandalism, terrorism and security in urban public passenger transport.* Economic Research Centre. Paris, France (ECMT Publications are distributed by: OECD Publications Service, 2, rue André Pascal, 75775 PARIS CEDEX 16, France.) Available at: https://www.itf-oecd.org/sites/default/files/docs/03rt123e.pdf.

Mailer, G. (2006). Individual perceptions and appropriate reactions to the terrorist threat in America's public spaces. In J. Forest (Ed.), *Homeland security: Protecting America's targets, volume II: Public spaces and social institutions*. Westport: Praeger Security International.

Public-Private Partnerships: Port Security

Pierre-Luc Pomerleau
Business Administration – Homeland Security and Leadership Policy, Northcentral University, San Diego, CA, USA

Keywords

Port security · Port threats · Public-private partnerships · Information sharing · Critical infrastructure · Supply chain · Security networks

P

Definition

Port security refers to security and law enforcement measures employed to safeguard port assets (vessels, harbors, facilities, cargos, employees, visitors) from natural and man-made threats, as well as from criminal activities.

Introduction

The security of maritime transportation is essential for the international economic well-being and as such is one of the subsectors in the critical

infrastructure. Critical infrastructure refers to a vital system that performs a specific function in society, "whose cessation or destruction would have a significant impact" (Curt and Tacnet 2018, p. 2441). According to the United Nations Conference on Trade and Development (2017), 80% of global trade by volume and more than 70% by value is carried on ships and handled by seaports worldwide (p. 61). Mega ports across Asia, North America, and Europe provide the primary maritime system for most of the world. Maritime shipping, like other transportation systems, faces several challenges in establishing and maintaining the access controls needed to secure shipments near a port, in port, or in transit from a port (Purpura 2008). In particular, ports must facilitate legitimate trade while at the same time protecting their assets against a myriad of threats.

Challenges in meeting the security needs of ships stem from two interconnected sources. First, the public and private sectors are responsible for monitoring the large volume of cargo transported internationally by ships. Second, in order to make a profit, this cargo must be transported quickly and efficiently. Even though ports are more secure today, they are still vulnerable due to their economic importance, the speed of shipping, and their visibility, and despite the maritime sector's vulnerability to natural and man-made threats, it has not received the same attention as other transportation sectors, due primarily to the small number of security incidents that have been made public.

After 2001, the maritime support system, including its ports and ships on the ocean, was determined to be a particularly attractive target because of its importance to the global supply chain of goods, its vulnerability due to gaps in security, and its strategic importance (Mat Salley 2006). Governments, law enforcement, intelligence agencies, and the private sectors of many nations realized that new threats to the maritime transportation mode were evolving at a rapid pace. For example, Bowley (2013) argues that a significant attack on one or more of the large mega-ports capable of servicing large vessels could cause substantial disruptions to international trade by impacting the current "just-in-time" business principle. The possibility of losing access to even one major port for several days would be highly problematic for the USA as it would affect not only the local area, private businesses locally and abroad but also the federal government (Government Accountability Office 2007).

The United States' borders include not only the southern border with Mexico and the northern border with Canada but also different areas of liquid borders between ports of entry in the Great Lakes as well as along the Pacific and the Atlantic oceans (Subcommittee on Border and Maritime Security 2011). The U.S. Coast Guard (USCG) is responsible for securing these borders, stopping drug trafficking, and performing other essential missions. The maritime system, however, is global and requires transnational cooperation to secure it against various threats – the U.S. Customs and Border Protection currently has 54 memorandum of understanding (MOU) with multiple partners (Government Accountability Office 2018). Meeting these threats is possible only through public and private partnerships (PPP) as neither public nor private entities fully control security at ports. Specifically, both the public and private sectors must work together "to establish a common scope, objectives and a working methodology to achieve shared goals" (The International Centre for the Prevention of Crime 2018, p. 141).

Port Security

Ports are both unique and complex as they often involve government-owned operations, private terminal operators, and other organizations that lease port authority facilities. This variety of ownership makes security complicated. As Brewer (2014) argues, the public and private "nodes" of each of these infrastructures have distinct interests, duties, responsibilities, and powers in policing the waterfront and the port. Traditional methods of crime prevention are not well suited to this context and a collaborative approach involving police, governments, and the private sector is necessary. Effective public-private sector coordination is vital to achieving resilience in maritime port security (Busch and Givens 2014).

Port Threats

In the modern era, traditional port crimes such as smuggling, piracy, and theft have been joined by other types of offenses – sabotage, labor unrest, insider threat, cyber-threat, stowaways, tampering with shipping containers, and leaving a dangerous item on a dock, as well as smuggling a weapon of mass destruction and other forms of terrorist acts (Brewer 2014; Christopher 2015; Government Accountability Office 2016; McNicholas 2016; Washington Post 2014). According to Fennelly et al. (2017), because most of the global trade consists of raw materials, controlled products, food, automobiles, clothing, and electronics, moving it by sea is the most effective way to proceed. However, this mode of transport relies on high volume, which creates challenges for the governments and private organizations responsible for ensuring safe and secure cargo. For instance, in the USA, only about 4% of cargos are inspected at seaports, while in Canada, it is only 2% (Quigley et al. 2017). This low percentage of inspection creates a major vulnerability for organized crime to exploit.

As an examination of all threats is beyond the scope of this chapter, only four of the threats seaports are currently facing are further examined here – terrorist threats, natural threats, insider threats, and cyber-threats. While terrorist and natural threats to maritime and port security have been discussed in the literature, cyber- and insider-threats are relatively new threats to law enforcement and must be carefully considered by port security management.

Terrorist and Natural Threats

Since 9/11, the threat of terrorism has forced ports to invest considerable amounts of money in security measures. However, although the probability of problems due to natural disasters and climate change is greater than the threat of terrorism such as the use of explosives or bombs to generate fear among the population, ports are not as prepared as they should be to maintain their operations when faced with such challenges. The Coast Guard is accustomed to guarding against cargo theft, drug smuggling, human trafficking, and stowaways. However, port security management teams and their law enforcement partners must also have emergency management and response plans in place to protect people and facilities from future natural threats as well as terrorism (Maritime Executive 2011).

Climate change will be a significant natural threat to ports in the future as changes in water level, storms, precipitation, and higher temperatures are likely to affect them directly (U.S. Environmental Protection Agency 2008). Threats from hurricanes include high winds, heavy rainfall, storm surge, coastal and inland flooding, and rip currents, as well as tornadoes – the 2005 hurricane season, which included Katrina, Rita, and Wilma – was particularly challenging for ports (Government Accountability Office 2007). It is already clear that natural events not only cause loss of life but also have a significant economic impact on ports – the total cost of damages for the Port Authority of New York and New Jersey from Hurricane Sandy in 2012 has been estimated at US$ 2.2 billion (Quigley et al. 2017). On a positive note, when hurricane Maria hit Puerto Rico in 2017, port operations were more resilient in maintaining functional operations, evaluating cargo shipments, and scanning incoming containerized cargos (Odegaard 2018). After only 36 h, the port operation was back to normal operations (Odegaard 2018).

Communication, interpersonal coordination, and interagency coordination are the three most common problems during natural disasters (Government Accountability Office 2007). Two best practices to ensure people know what to do and how to react to a natural or man-made crisis are having updated emergency management plans and conducting tabletop exercises to practice emergency situations with stakeholders to assess the ability of different government agencies and business entities to respond to and recover from a crisis (U.S. Department of Homeland Security 2005).

Cyber-Threats

Effective information and communications technology are vital to protecting maritime and port

infrastructure (Willis 2016). Logistics systems rely on technology to monitor the flow of shipments as well as transactions among manufacturers, carriers, and shipping organizations. Vessel navigation depends on the global positioning system and automated control systems are now an important part of the port infrastructure, for example, in shipment navigation, natural gas transportation, oil loading or unloading, and electric grids. However, the technologies that increase efficiency in maritime transportation also heighten the system's vulnerability to cyberattacks as these systems can be exploited to disrupt port operations or to damage port infrastructure (Willis 2016). Navigation or control systems can be hacked, increasing the risk of vessel collisions, and the integrity of data control systems can be compromised so that manifest information cannot be trusted (Willis 2016). Some examples of cyber-threats for ports are the risk of having a cyberattack against servers, phishing and spear-phishing attacks, zero-day exploits, or man-in-the-middle (session hijacking) attacks among others.

Besides, according to the International Maritime Bureau (IMB), there is a real danger that emails being sent to and from ships are monitored or altered, thus potentially affecting commercial transactions. Many vessels are still using outdated computer software that has not been designed with cybersecurity in mind, exposing ships to cyberattacks (Bull 2016). Willis (2016) questions whether the current protection and redundancies in place to mitigate these vulnerabilities are sufficient, and if it is clear, who is to respond to any cyberattack on port infrastructure in the future.

Cyberattacks on the maritime transportation system can result in loss of life, physical damage to critical infrastructure, disruption of supply chains, and theft of sensitive information, as well as being used to support criminal organization activities such as cargo smuggling or cargo theft (Transport Canada 2016). In June 2017, Maersk, the world largest container shipping company was the victim of a cyberattack that demonstrated the scale of damage a computer virus can create in an interdependent and interconnected industry (Saul 2017). This cyberattack was the most critical disruption of the global shipping industry to date as several ports operated by Maersk in the USA, India, Spain, and the Netherlands were unable to conduct business. The company was forced to shut down its computer systems to carry out a forensic investigation, which meant that, since the global positioning systems were not functioning, it no longer knew where its containers were, increasing the possibility of further loss and/or theft (Saul 2017).

To prevent a similar situation, shipping companies should conduct joint cybersecurity vulnerability assessments with law enforcement to assess their computer systems and evaluate the risk of any type of cyber-related attacks. Companies should have an updated recovery plan and governance and oversight of their security programs should be implemented by a cybersecurity committee, which should also review their access controls and computer network design, updating (or installing) an intrusion detection system and securing all communications through encryption (Transport Canada 2016).

Insider Threat

Managing and detecting employees at risk of committing internal criminal conspiracies is a complex challenge for seaports (Christopher 2015). Catrantzos (2012) defines an insider threat as "an individual and, more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust in or with the infrastructure being targeted" (p. 4). Port employees may help members of organized crime groups to smuggle drugs or instruments of terror as part of legitimate cargo traveling on commercial vessels and cruise ships or may remove contraband material or conceal it before it can be detected by U.S. Customs and Border Protection or technological detection systems (Christopher 2015). When using cargos as a mean to transport drugs, organized crime almost always relies on the assistance from port employees. In 2018, authorities working at the Port of Rotterdam in the Netherlands and the Port of Antwerp in Belgium seized more than 73 metric tons of cocaine, a 35% increase from

the year before (Den Held and Asmann 2019). According to Den Held and Asmann (2019), corrupt workers at the Port of Antwerp earned between EUR 75,000 and EUR 125,000 per drug shipment.

Those who pose an insider threat may have other motives, such as helping to launch cyber- or physical-security attacks on the maritime global supply chain (Shapiro et al. 2018). Ports and naval employees may also be interested in aiding state or non-state actors who want to disrupt national security or critical infrastructure operations either for personal economic gain or to lead to a loss of revenue for private and public organizations (Shapiro et al. 2018). A recent risk is the threat of homegrown violent extremism (Cozine 2019). For example, a radicalized employee working at a port or a visitor of the port could be a threat to the security of the port operations, the safety of employees, and assets in the event that a terrorist attack would be perpetrated in a port area. Screening employees and visitors through background checks is key in risk management. Being able to identify individuals who show signs of radicalization or extremist behaviors and characteristics is also essential for law enforcement professionals working at ports (see chapter on ▶ "Border Security" in this volume).

The Importance of the Supply Chain

Most criminal activities carried out by transnational criminal organizations using ships and containers to exploit vulnerabilities within the maritime supply chain are very lucrative. On average, 675 shipping containers are lost or stolen at sea each year, which has substantial consequences for the finances and reputations of private organizations (World Shipping Council 2017).

Fennelly et al. (2017) argue that supply chain security in the future will be tied to what they refer to as the sea lines of communications (SLOCs) which, as the focus of maritime security, will affect ports, shipping lanes, chokepoints, and coastal waters as the ability to move goods quickly and securely will continue to be paramount for global commerce. SLOCs will bring about a shift in regulations, with an emphasis on supply chain and cargo security leading to a change in the present focus on port security. This systemic approach will be possible due to significant developments in technology that will provide improved methods of tracking, smart locks, and information databases, allowing cargo to move through the supply chain quickly, securely, and efficiently. It will also make it possible to identify cargo loads operating outside the regular security pipelines (Fennelly et al. 2017). To comply with federal regulations and controls, shipping companies will rely on specialized examinations and testing to certify cargo ships before they sail (O'Brien 2015).

Law Enforcement Initiatives

Different strategic initiatives to improve security and share intelligence have been implemented over the years. The Shiprider program is an excellent example of work that is being done across the US/Canadian border with the assistance of the Royal Canadian Mounted Police (RCMP), as is the integrated 2006 Cross-borders Maritime Law Enforcement Operations (ICMLEO, Royal Canadian Mounted Police 2016). The Coast Guard's Deployable Operations Group illustrates the role that maritime, port security, and specialized naval teams play in the Coast Guard's post 9/11 mission. This group was created in 2007 as a domestic maritime counter- and anti-terrorism force against threats at home and abroad and brings together organizations such as port security, tactical law enforcement teams, maritime safety units, and security response teams (Subcommittee on Border and Maritime Security 2011; Lowe 2016). For example, this group was deployed for the 2010 earthquake in Haiti and in the piracy mission of the 2009 Maersk Alabama hijacking case on the African coast (Lowe 2016).

Public-Private Partnership Initiatives

Many initiatives have been undertaken by public and private partners to enhance port and maritime

security. The Container Security Initiative (CSI) that examines high-risk, US bound, containerized cargos at foreign ports, the 24-h rule that requires that freight manifests be submitted at least 1 day before shipment arrivals, and the 96-h rule (prior to arrival) for ships bound for US maritime ports are excellent examples of initiatives aimed at protecting ports and increasing maritime security (Busch and Givens 2014; Christopher 2015). The Coast Guard has worked with Microsoft to produce an electronic chip that allows ship's crews to enter information in computers while they are at sea and offline and then transmit this data to the Coast Guard. As such, it keeps the Coast Guard informed of the ships' positions at sea once they have access to the Internet, increasing the efficiency of security operations and the productivity of crew members (Busch and Givens 2014).

The Customs-Trade Partnership Against Terrorism (C-TPAT) initiative, which works voluntarily with the Customs and Border Protection agency to undertake inspections for US importers, is another example of a partnership that has increased transparency in the supply chain, helping to identify suspicious shipments (Government Accountability Office 2016; Maritime Executive 2011). The Transportation Worker Identification Card program helps screen employees and individuals who have access to critical port infrastructure (Willis 2016), and the X-ray, gamma-ray, and radiation detection systems at ports have contributed to reducing the risk that different types of bombs and radiological materials will be shipped in inbound cargo containers (Maritime Executive 2011; Willis 2016).

Another example of an excellent public and private partnership initiative is the creation of the Maritime Security Council, which developed an Information Sharing and Analysis Center (ISAC) composed of public and private actors representing maritime port employees from around the world. Representatives from both sectors work alongside each other, fostering collaborations that produce information essential to decision-making. This type of PPP initiative or fusion center facilitates information-sharing between maritime port security stakeholders such as the U.S. Coast Guard and various private entities (Busch and Givens 2014). In their study of Australian fusion centers, Bright and Whelan (2018) argue that the "hub-and-spoke" model should be prioritized in sharing information for national security and law enforcement purposes. This model has a primary center that acts as a central "hub," while various Joint Analyst Groups (JAGS) – multiagency groups located in major jurisdictions or regional fusion centers – are connected to the central hub (Bright and Whelan 2018).

As it is common in the protection initiatives of different industries and with regard to critical infrastructure, port security professionals should use data analytics techniques, such as machine learning, to identify possible common denominators, suspicious activities, or anomalies in employee's behaviors to detect potential insider threat as well as any potential criminal activities (see chapter on ▶ "Machine Learning" in this volume). Data is critical in managing security, and data analytics for port security is no different than that dealing with other critical assets. Data analytics techniques make it possible to learn continually from port security data by focusing primarily on high-risk behaviors and anomalies while prioritizing financial resources, efforts, and costs in mitigating port security risks, as well as using data sets to create rules and models that reduce false positives. Security analysts should rely on real-time data that allow them to create a detailed threat assessment by pulling relevant and valuable data from multiple sources (e.g., scanning data, employee data, information logs, security logs), making it possible to conduct targeted and risk-based security assessments (Odegaard 2018). The use of data analytics should be explored further to understand how it can be used to manage various threats, such as those posed by gaps in cybersecurity or criminal insiders, and to improve port security.

How Private and Public Partnerships Could Improve Port Security Going Forward

Various modes of crime controls and incidents may be part of the future of maritime

transportation (Brewer 2014). To increase efficiency, the traditional and rigid hierarchical structure presently used to manage security needs to be replaced by a horizontal structure that is more flexible, fluid, and adaptable to the level of complexity now found in criminal organizations (Cozine et al. 2014; Gerspacher and Dupont 2007). New legislation may be necessary to allow law enforcement and public entities to work more closely with the private sector. For example, the public sector has the power to enforce the law, but the private sector has access to an enormous quantity of data that is needed to prevent crime and terrorism. The private sector also has skills and financial and human resources that the public sector lacks. Private sector professionals with skills in data analytics, computer science, or cybersecurity should be leveraged to improve the overall security of ports by combining their work with the strengths and knowledge of the public sector.

The flexible networks now being used by organized crime and terrorist groups give them a competitive edge (Gerspacher and Dupont 2007). A horizontal organization in port security would promote increasing trust between member organizations, encouraging better information-sharing capabilities and lower operating costs than the conventional vertical integrated structures used by most agencies and private companies today (Dupont 2015). Trust between public and private organizations is critical to trans-governmental cooperation and to meet cross-jurisdictional challenges such as combating terrorism and transnational crime (Cozine et al. 2014).

As argued by Dupont (2015), legitimate networks will have to adopt and mirror the structure of organized crime networks if they hope to be successful in countering their actions. These future networked systems will have to build layers of protection and defense-in-depth structures if they are to deal effectively with critical system security risks while preserving flexibility, functionality, and efficiency (U.S. Department of Homeland Security 2005).

Future security networks will also need to emphasize the importance of cooperation and participation between both domestic and international stakeholders as well as making sure that each partner uses their expertise to manage strategic points (U.S. Department of Homeland Security 2005). According to Brewer (2014), protecting ports from crime and natural disasters will require mobilizing public and private actors in highly connected security networks that demonstrate trust in their peers, build social capital, and engage in activities of co-production towards the same common objectives. More specifically, networks of public and private actors could work together to plan joint investment projects in digital technology as well as employee training (e.g., protection techniques, vulnerability assessment). The same networks should also collaborate in audits and inspections and in creating new standards for port security when responding to man-made and natural crises, as well as co-creating new types of technological security software and hardware to improve port and maritime security.

The private sector might take the lead in providing security and video surveillance at ports, which would allow the public sector to allocate more resources to other priorities for port and maritime security. The private sector could also bring new security skills, such as techniques like crime prevention through environmental design (CPTED), to enhance physical security and access controls while the public sector would continue to be responsible for enforcing the law.

The private sector could assist public sector port authorities in using data analytics to improve their intelligence, enabling them to better detect insider threats, as well as with computer science and encryption skills that would help them work with law enforcement to mitigate cybersecurity threats to ports, communications, cargos, and vessels. Increased intelligence would also facilitate crucial decisions such as the deployment of personnel and the use of automated processes (Odegaard 2018).

Furthermore, if intelligence is accumulated in a fusion center such as an ISAC, data can be gathered in one platform, aggregated, analyzed, and more easily disseminated to the right individuals. This approach would enhance collaboration in using data from both internal and external services to create an optimal intelligence

cycle for public-private partnership security networks (Odegaard 2018). Finally, the private sector might also assist in improving security at ports by developing innovative biometric capabilities as well as the use of satellite imagery or unmanned aerial vehicles.

Conclusion

The digital evolution of our globalized economy will continue to progress and change rapidly. This progress will bring more challenges and new risks. Cybersecurity and insider threat risks will significantly increase the economic and national security challenges for ports and maritime security as well as other critical infrastructures. Adversaries will employ different sophisticated technological tools and substantial financial resources to achieve their criminal goals. Like governments, the private sector and public law enforcement will have to adapt and deal with these threats in a context of limited resources. It will thus be imperative for security and law enforcement professionals to use a risk-based approach in making decisions and choosing strategies as prevention measures and technological controls are extremely expensive to deploy, difficult to implement, and to maintain.

Crime-control partnerships between public and private actors have often been implemented to provide physical security and access control, and the same approach must be taken to manage cyber and technological threats. Digital networks using secure online communications to share intelligence about threats towards ports should be given priority. Moreover, governments should continue to encourage the private sector to design security hardware and software that promotes security (Yang 2010). The efficiency of public-private partnerships should be quantified through evaluation plans that assess the overall performance of such partnerships based on measurable objectives, key performance indicators, and evaluation methodologies, which will facilitate the implementation of future partnership programs (Government Accountability Office 2018).

The security measures established since 2001 through public and private partnerships and new legislation have improved port security while maintaining port efficiency (Willis 2016), but ports are still significant targets for man-made and natural threats, and there are still challenges in information sharing. More emphasis should be given to protecting national security, the economy, and people. To succeed in this strategic objective, partnerships between various public and private actors will be vital to mitigating future risks.

Cross-References

- ▶ Border Security
- ▶ Machine Learning
- ▶ Maritime Security: Armed Guards on Board
- ▶ Maritime Security: Problems of Security Versus Safety Practices
- ▶ Natural Hazards: Hurricanes, Cyclones, and Typhoons
- ▶ Physical Security: Interior Applications
- ▶ Police: Public Versus Private Policing
- ▶ Public-Private Partnerships: Security Organizations
- ▶ Terrorism: Domestic
- ▶ Terrorism: International

References

Bowley, R. (2013). *Countering terrorism in the maritime domain: A contemporary evaluation of the international legal framework*. Ph.D. Dissertation. University of Wollongong. Retrieved from http://ro.uow.edu.au/theses/4262/

Brewer, R. (2014). Policing the waterfront; networks, partnerships, and the governance of port security. Retrieved from https://www.amazon.com/Policing-Waterfront-Partnerships-Governance-Criminology/dp/0199687366

Bright, D., & Whelan, C. (2018). On the relationship between goals, membership and network design in multi-agency "fusion" centres. *Policing: An International Journal of Police Strategies and Management*. https://doi.org/10.1108/PIJPSM-05-2018-0070.

Bull, K. (2016). Maritime companies warned of cyber attacks. Retrieved from https://www.securitymagazine.com/articles/87391-maritime-companies-warned-of-cyber-attacks

Busch, E. N., & Givens, D. A. (2014). The business of counterterrorism: Public–private partnerships in

homeland security. Retrieved from https://www.amazon.com/Business-Counterterrorism-Public-Private-Partnerships-Terrorism/dp/1433119544

Catrantzos, N. (2012). Managing the insider threat: No dark corner. Retrieved from https://www.amazon.com/Managing-Insider-Threat-Dark-Corners/dp/1439872929

Christopher, K. (2015). Port security management. Retrieved from https://www.amazon.ca/Port-Security-Management-Kenneth-Christopher/dp/1466591633/ref=sr_1_1?s=books&ie=UTF8&qid=1548502307&sr=1-1&keywords=port+security+management

Cozine, K. (2019). Border security. In L. Shapiro & M. H. Maras (Eds.), *Encyclopedia of security and emergency management*. Cham: Springer.

Cozine, K., Joyal, R. G., & Ors, H. (2014). From local to global: Comparing network approaches to addressing terrorism and transnational crime. *Journal of Policing, Intelligence and Counter Terrorism, 9*(2), 117. https://doi.org/10.1080/18335330.2014.940817.

Curt, C., & Tacnet, J. (2018). Resilience of critical infrastructures: Review and analysis of current approaches. *Risk Analysis: An International Journal, 38*(11), 2441–2458. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.13166

Den Held, D., & Asmann, P. (2019). Colombia cocaine boom likely behind rising European port seizures. Retrieved from https://www.insightcrime.org/news/analysis/colombia-cocaine-boom-rising-seizures-europe-ports/

Dupont, B. (2015). Security networks and counter-terrorism: A reflection on the limits of adversarial isomorphism. In M. Bouchard (Ed.), *Social networks, terrorism, and counter-terrorism* (pp. 155–174). New York: Routledge. Retrieved from http://tsas.ca/fr/tsas_library_entry/security-networks-and-counter-terrorism-a-reflection-on-the-limits-of-adversarial-isomorphism/

Fennelly, J. L., Beaudry, M., & Perry, A. M. (2017). Security in 2025. Retrieved from https://www.asisonline.org/ASIS-Store/Products/Pages/Security-in-2025.aspx

Gerspacher, N., & Dupont, B. (2007). The nodal structure of international police cooperation: An exploration of transnational security networks. *Global Governance, 13*(3), 347–364. Retrieved from https://www.jstor.org/stable/27800666?seq=1#page_scan_tab_contents

Government Accountability Office. (2007). Port risk management; additional federal guidance would aid ports in disaster planning and recovery. Retrieved from https://www.gao.gov/new.items/d07412.pdf

Government Accountability Office. (2016). Maritime security: Progress and challenges in implementing maritime cargo security programs. Retrieved from https://www.gao.gov/products/GAO-16-790T

Government Accountability Office. (2018). U.S. port of entry; CBP public–private partnership programs have benefits, but CBP could strengthen evaluation efforts. Retrieved from https://www.gao.gov/products/GAO-18-268

International Centre for the Prevention of Crime. (2018). Sixth international report on crime prevention and community safety: Preventing cybercrime. Retrieved from http://www.crime-prevention-intl.org/en/publications/report/report/article/6th-international-report-on-crime-prevention-and-community-safety-preventing-cybercrime.html

Lowe, C. (2016). These are the Coast Guard's special operations forces. Retrieved from http://www.wearethemighty.com/articles/these-are-the-coast-guards-special-operations-forces

Maritime Executive. (2011). 10 Years after 9/11, security still a top priority of U.S. ports. Retrieved from https://www.maritime-executive.com/article/10-years-after-9-11-security-still-a-top-priority-of-u-s-ports

Mat Salley, N. (2006). Post 9/11 maritime security measures: Global maritime security versus facilitation of global maritime trade. Master's Dissertation. Retrieved from https://commons.wmu.se/cgi/viewcontent.cgi?referer=https://www.google.ca/&httpsredir=1&article=1097&context=all_dissertations

McNicholas, M. (2016). Maritime security: An introduction. Retrieved from https://www.amazon.ca/Maritime-Security-Second-Introduction-McNicholas/dp/B01FIY1H6S/ref=sr_1_1?ie=UTF8&qid=1549289310&sr=8-1&keywords=maritime+security+an+introduction+second+edition

O'Brien, B. (2015). Three hazards of shipping by sea and how to avoid them. Retrieved from http://www.tradeready.ca/2015/trade-takeaways/three-hazards-shipping-by-sea-avoid/

Odegaard, M. (2018). Port of San Juan: A case study in port security innovation. Retrieved from https://www.marinelink.com/news/port-san-juan-a-case-study-port-security-441624

Purpura, P. P. (2008). *Security and loss prevention: An introduction*. Amsterdam: Elsevier.

Quigley, K., Bisset, B., & Mills, B. (2017). Too critical to fail: How Canada manages threats to critical infrastructure. Retrieved from https://www.amazon.ca/Too-Critical-Fail-Manages-Infrastructure/dp/0773551611/ref=sr_1_1?s=books&ie=UTF8&qid=1548361193&sr=1-1&keywords=too+critical+to+fail

Royal Canadian Mounted Police. (2016). Canada–U.S. Shiprider. Retrieved from http://www.rcmp-grc.gc.ca/ibet-eipf/shiprider-eng.htm

Saul, J. (2017). Global shipping feels fallout from Maersk cyber attack. Retrieved from https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE

Shapiro, L. R., Maras, M.-H., Velotti, L., Pickman, S., Wei, H.-L., & Till, R. (2018). Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security, 11*(3/4), 65. Retrieved from https://link.springer.com/article/10.1007/s12198-018-0191-3

Subcommittee on Border and Maritime Security. (2011). Securing the nation's ports and maritime border – A review of the coast guard's post-9/11 homeland security mission. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72241/pdf/CHRG-112hhrg72241.pdf

Transport Canada. (2016). Understanding cyber risks: Best practices for Canada's maritime sector. Retrieved from http://publications.gc.ca/collections/collection_2016/tc/T86-21-2016-eng.pdf

U.S. Department of Homeland Security. (2005). Maritime transportation system; Security recommendations for the national strategy for maritime security. Retrieved from https://www.dhs.gov/sites/default/files/publications/HSPD_MTSSPlan_0.pdf

U.S. Environmental Protection Agency. (2008). Planning for climate change impacts at U.S. ports. Retrieved from https://archive.epa.gov/sectors/web/pdf/ports-planing-for-cci-white-paper.pdf

United Nations Conference on Trade and Development. (2017). Review of maritime transport 2017. Retrieved from https://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf

Washington Post. (2014). Safeguarding America's seaports from terrorism. Retrieved from https://www.washingtonpost.com/politics/federal_government/safeguarding-americas-seaports-from-terrorism/2014/11/11/c4a17e1c-69b4-11e4-b053-65cea7903f2e_story.html?utm_term=.829dfec623b0

Willis, H. H. (2016). Ten years after the Safe Port Act, are America's ports secure? Retrieved from https://www.rand.org/blog/2016/04/attractive-targets.html

World Shipping Council. (2017). Containers lost at sea – 2017 update. Retrieved from http://www.worldshipping.org/industry-issues/safety/Containers_Lost_at_Sea_-_2017_Update_FINAL_July_10.pdf

Yang, C. Y. (2010). Impact of the container security initiative on Taiwan's shipping industry. *Maritime Policy and Management, 37*(7), 699–722. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/03088839.2010.524737.

Further Reading

Bright, D., & Whelan, C. (2018). On the relationship between goals, membership and network design in multi-agency "fusion" centres. *Policing: An International Journal of Police Strategies and Management*. https://doi.org/10.1108/PIJPSM-05-2018-0070.

Christopher, K. (2015). Port security management. Retrieved from https://www.amazon.ca/Port-Security-Management-Kenneth-Christopher/dp/1466591633/ref=sr_1_1?s=books&ie=UTF8&qid=1548502307&sr=1-1&keywords=port+security+management

Direnzo, J., Drumhiller, K. N., & Roberts, S. F. (2017). Issues in maritime cyber security. Retrieved from https://www.amazon.ca/Issues-Maritime-Cyber-Security-Roberts/dp/1633915557/ref=sr_1_1?s=books&ie=UTF8&qid=1521228638&sr=1-1&keywords=issues+in+maritime+cyber+security

Quigley, K., Bisset, B., & Mills, B. (2017). Too critical to fail: How Canada manages threats to critical infrastructure. Retrieved from https://www.amazon.ca/Too-Critical-Fail-Manages-Infrastructure/dp/0773551611/ref=sr_1_1?s=books&ie=UTF8&qid=1548361193&sr=1-1&keywords=too+critical+to+fail

Public-Private Partnerships: Security Organizations

Christopher Cleary
St. John's University, New York, NY, USA

Keywords
NYPD Shield · FBI InfraGard

Definition

Public-private partnership (PPP) information sharing networks are communication networks that enable the flow of security and threat information between public sector law enforcement agencies and private sector businesses. The networks are mutually beneficial efforts combining the resources of all participating entities to provide a unified and coordinated defense against potential hazards and threats.

Introduction

Security professionals must guard against a long and evolving list of potential threats and hazards. Some security problems such as theft, unlawful violence, and natural disasters have been present throughout recorded history. Other serious problems such as cyberthreats have recently emerged but pose significant security challenges.

Providing protection against all potential natural, accidental, and intentional threats and dangers cannot be accomplished by any single private or governmental entity. Combining the resources of both sectors has proved to be a mutually beneficial method to enhance capabilities. In their report on information sharing, the Department of Justice recognized the need to collaborate, saying, ". . .neither law enforcement nor private security can protect the nation's infrastructure alone, law enforcement-private security partnerships are essential to bridging the gap" (US Department of Justice 2005).

Public sector law enforcement agencies referenced in this paper include federal, state, tribal, and local entities that provide policing or investigative services. It is estimated that there are over 18,000 state and local law enforcement agencies in the USA employing more than 600,000 sworn members (US Department of Justice 2016).

Private sector entities referenced in this paper include for-profit and not-for-profit corporations, businesses, agencies, and organizations. The security for these entities may be the responsibility of:

- A commercial security firm contracted to provide security to a private entity.
- A security specialist employed by a private entity to improve security and disaster planning.
- A business owner or employee who is not a security specialist but has the responsibility for security and disaster planning.

It is estimated that there are over 1.1 million private security officers in the USA (US Department of Labor 2017). The total number of individuals involved in security-related decision-making in the US private sector is unknown but can be assumed to be higher.

The resources from both the public and private sectors that are tasked with preventing crime and maintaining homeland security are significant, but collaboration greatly increases their effectiveness. There has been increase in collaboration through the implementation of information-sharing networks designed to safeguard cyber networks and critical infrastructure locations and to protect against acts of terrorism.

Collaboration

Private sector entities provide for the security of their physical property and proprietary assets but rely on public sector services to fill gaps that are beyond their abilities. Private sector security might lawfully detain a subject for committing a trespass upon their company property but rely on local police and the district attorney to process the arrest and prosecute the offender. Public sector agencies are limited by having finite resources that are insufficient to provide comprehensive security for every potential target of illegal activity or disaster within their jurisdiction. State, tribal, and local police agencies provide general patrol coverage within their jurisdiction but don't have the staffing necessary to post police officers at every critical location, such as facilities operated by small businesses, electric power utilities, drinking water providers, communications companies, or the financial sector. Public sector entities must rely upon the private sector to provide specialized equipment and expertise that may not be available in the public sector, as well as in-depth knowledge of their proprietary locations.

While public and private entities develop their individual plans to increase preparedness and resilience, the plans are likely incomplete unless they include cooperation agreements or understandings with other entities to fill in gaps. Individual plans must be coordinated with other agencies or entities that are expected to play a role in the plan (Federal Emergency Management Agency 2010, pp. 1–7). Collaboration is a key component to developing a comprehensive security plan.

After the terror attacks of September 11, 2001, information sharing was recognized as a key component of cooperative collaboration to defend the nation against acts of international terrorism. In their Final Report, the 9/11 Commission noted:

> ". . .the private sector controls 85 percent of the critical infrastructure of the nation. Indeed, unless a terrorist's target is a military or other secure government facility, the "first" first responders will almost certainly be civilians. Homeland Security and national preparedness therefore often begins with the private sector." The commission further noted that "Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security." (9/11 Commission 2004, p. 397)

Information Sharing

Many criminal justice agencies at the federal, state, and local levels recognized the importance of sharing information across jurisdictions and

across disciplines to develop a common operational picture. Public sector law enforcement agencies have access to the most current intelligence which is needed by, but may be inaccessible to, private sector security providers. Private sector entities have in-depth knowledge and expertise of their own industry and their own facilities. Private sector entities will also have knowledge about suspicious activities that do not reach a reporting threshold but would be of interest to law enforcement, such as irregular purchases of components used to construct improvised explosive devices like commercial fertilizer or concentrated peroxide.

The National Criminal Intelligence Sharing Plan provides policy recommendations for criminal justice agencies to establish information sharing as an essential function of policing strategy and states "Law enforcement agencies should consider creating and implementing outreach strategies in order to develop and enhance partnerships with the private sector, nonlaw enforcement public safety disciplines, privacy advocates, and community groups" (US Department of Justice 2013, p. 17).

While there are many benefits to participation in a public-private network, sharing information between public and private entities is a complex problem. Sharing data that was collected by the US intelligence community has the potential to expose, and thereby render ineffective, valuable collection capabilities or assets, including the ability to intercept electronic communications, or human intelligence assets (covert operatives and confidential informants). Information or data collected by covert collection methods that has been processed and analyzed into intelligence products will likely be designated Classified National Security Information, which prevents its dissemination to anyone without a government issued security clearance (Executive Office of the President 2009). A large percentage of the information held by law enforcement agencies relates to criminal cases, the release of which would likely make further investigation and prosecution of the cases difficult or impossible. Additionally, criminal justice agencies often possess sensitive information about citizens (identification of crime victims, medical or psychiatric records) which should not be divulged without legal authorization.

Private companies face serious issues of trust, control, and disclosure while deciding whether to share information with the public sector. Sharing information about a criminal occurrence, such as a cyber intrusion, might result in the company losing control of their own investigation or of sensitive proprietary information being made public. Even though a cyber intrusion might cause serious damage, the company might decide that reporting the intrusion might result in greater damage to the company's image or reputation (Hernandez 2017).

To encourage the private sector to share sensitive information, many PPP networks utilize privacy protection guidelines. The Traffic Light Protocol (TLP) is one example of a privacy protection guideline. TLP uses a four-color system to help ensure that proprietary or sensitive information is only shared with the "proper audience." Sources may use:

- TLP: Red when dissemination of the information could cause damage to an entity's privacy, reputation, or operation, and it cannot be acted upon by other entities.
- TLP: Amber can be used when dissemination of the information could cause damage to an entity's privacy, reputation, or operation, but requires support to be acted upon.
- TLP: Green can be used when the information could be useful if disseminated to all partner organizations within the sector or network.
- TLP: White can be used to identify information that can be disseminated freely with little or no foreseeable negative effect (US Department of Homeland Security 2016a, p. 14).

Critical Infrastructure Protection

In 2013, a Presidential Policy Directive identified 16 critical infrastructure sectors which are "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have

a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (Executive Office of the President 2013, p. 12).

The federally designated critical infrastructure sectors include the chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials as well as waste, transportation systems, and water and wastewater systems (Executive Order No. PPD-21 2013).

The FBI instituted the *InfraGard* network to facilitate the exchange of all-hazards information between the federal government and private sector agencies to protect the nation's critical infrastructure from acts of terrorism and other criminal activities. The InfraGard network was initiated in 1996 in the Cleveland Field Office and has grown into an alliance of 82 local chapters throughout the USA. Each chapter is composed of businesses, state, tribal, and local law enforcement agencies, and academic institutions controlled by a locally elected board of directors that ensures their specific information-sharing needs are met.

The goals of the InfraGard program are to:

- Improve communication and reporting between the FBI and InfraGard partners related to major crimes, cybercrimes, and hostile acts against the USA or US interests.
- Facilitate the quick dissemination of relevant threat advisories, alerts, and warnings.
- Increase liaison and sharing of information on threats with critical infrastructure and key resources providers and their interdependencies.
- Provide training and education opportunities for members on counterterrorism, counterintelligence, cybercrime, and other issues relevant to security and resilience.

To ensure the security of the information being shared, the FBI conducts a vetting investigation on prospective members. Once the investigation is completed, participants are permitted access to the secure members-only InfraGard website, which contains intelligence and informational products and publications and provides a pathway for members to provide notifications of suspicious activity back to the FBI for investigation or for informational purposes.

(Federal Bureau of Investigation 2018).

Counterterrorism Networks

The threat of terrorism continues to be one of the most serious challenges faced by security providers. The threat comes from individuals who are either directed to commit atrocities by a terror organization or by individuals acting on their own who have been inspired by a terroristic ideology. Security threats are posed by both foreign terror organizations and domestic extremist groups (Federal Bureau of Investigation 2017).

NYPD Shield is a web-based information-sharing network of police, first responder agencies, and private sector security providers that is primarily focused on sharing threat information to guard against acts of terror within the New York City region. Controlled and operated by the New York Police Department (NYPD) Counterterrorism Bureau, the network was created with the understanding that defending against terrorism is a shared responsibility that requires the active participation of both public and private sector agencies.

NYPD actively solicits participation from private sector agencies, businesses, and corporations. Potential members undergo a vetting process designed to protect the integrity of the network. Once approved, members are encouraged to use the network and the information provided therein to bolster their entities' security against and resilience to acts of terrorism and to act as a force multiplier in recognizing and reporting suspicious behavior.

The successful Shield program was awarded the Michael Shanahan Award for Leadership in Public/Private Cooperation by the International Association of Chiefs of Police and the Security Industry Association (International Association of Chiefs of Police 2015).

Members of the NYPD Shield network participants are provided with a variety of products and services related to preparedness and security including (New York Police Department 2018):

- Briefs and analyses of security issues related to upcoming special events, mass gathering locations, critical incidents, and acts of terror from around the world,
- Security-related guides and publications produced by NYPD on topics include recommendations for active shooter protocols, security recommendations for high-risk buildings, and in-depth analysis of terror groups,
- The weekly terrorism brief contains an overview of each week's most relevant incidents, trends, and policy issues related to domestic, homegrown, and international terrorism. The brief also highlights topical issues of global security which are not directly tied to terrorism.
- The CBRN weekly brief contains assessment of open-source incidents related to chemical, biological, radiological, and nuclear incidents and security.
- Corporate and private sector training, which is available on request to participating member organizations. The NYPD counterterrorism bureau provides training courses that are available on request and cover topics including terrorism awareness, suspicious mail and packages, vehicle-borne improvised explosive device checkpoints, and critical infrastructure protection.
- A resource library with links to information on best practices and safety and security recommendations regarding all-hazard threats for general and sector-specific users,
- Shield conferences, which are held periodically to provide members with presentations from subject matter experts discussing issues and incidents related to terrorism.

Cybersecurity Networks

Cybercrime has become one of the most predominant and dangerous threats to security. A cyberattack can result in valuable data to be stolen, destroyed, or held for ransom. Sophisticated intrusions have been perpetrated by foreign governments, criminal organizations, professional hackers, hacktivists, and terrorist organizations. According to the FBI, cyber intrusions intending to illegally access and steal classified information, trade secrets, technology, and ideas are continual and growing problem. Hackers are also constantly attempting to access and attack critical infrastructure which could cause significant harm to our economy (Federal Bureau of Investigation 2017).

Cybersecurity is an area that benefits greatly from combining resources through public-private partnerships. Many private sector entities use sophisticated and specialized methods to detect and prevent intrusions. The public sector is authorized to investigate cybercrimes and, when necessary, work with international agencies to develop intelligence about the cyberthreats (Hernandez 2017).

Since cybercrime has the potential to affect almost every aspect of security, most PPP information-sharing networks, regardless of their primary focus, share information on cyberthreats. However, there are networks solely dedicated to the protection of cyber assets. The Department of Homeland Security (DHS) is the lead federal department for protecting "whole-of-nation" critical infrastructure, including cyber assets and has developed and implemented numerous information-sharing programs designed to enhance network security:

- The National Cybersecurity and communications integration center (NCCIC) is designed to create shared situational awareness of malicious cyber activity across public and private sectors.
- The cyber information sharing and collaboration program (CISCP) is DHS's "flagship" program for public-private information sharing. Network partners share information about threats, incidents, and vulnerabilities.
- Enhanced cybersecurity services (ECS) is an intrusion detection and prevention capability that is available to public and private sector partners. It is a free service that protects networks against unauthorized access, exploitation, and data exfiltration.

- Automated Indicator sharing (AIS) allows the federal government and the private sector to exchange cyberthreat information at "machine speed" (US Department of Homeland Security 2016b).

Conclusion

Providing protection against all potential natural, accidental, and intentional threats and dangers cannot be accomplished by any single private or governmental entity. Combining the resources of both sectors has proved to be a mutually beneficial method to improve capabilities. Public-private partnership (PPP) information-sharing networks are communication networks that enable the flow of security and threat information between public sector law enforcement agencies and private sector businesses.

Cross-References

► Security: Concepts and Definitions

References

9/11 Commission. (2004). National Commission on terrorist attacks upon the United States. The 9/11 commission report. Washington, DC. https://www.9-11commission.gov/report/911Report.pdf

Domestic Security Alliance Council. (2008). Domestic security alliance council-about. https://www.dsac.gov/about

Executive Order No. 13526. (2009). Executive office of the President. Classified National Security Information. Federal register. https://www.federalregister.gov/documents/2010/01/05/E9-31418/classified-national-security-information

Executive Order No. PPD-21. (2013). Executive Office of the President. Critical infrastructure security and resilience. https://fas.org/irp/offdocs/ppd/ppd-21.pdf

Federal Bureau of Investigation. (2017). Current threats to the homeland. Statement before the senate homeland security and government affairs committee. Washington, DC. 27 Sept 2017. https://www.fbi.gov/news/testimony/current-threats-to-the-homeland

Federal Bureau of Investigation. (2018). InfraGard. https://www.fbi.gov/about/partnerships/infragard

Federal Emergency Management Agency. (2010). Developing and Maintaining Emergency Operations Plans. https://www.fema.gov/media-library-data/20130726-1828-25045-0014/cpg_101_comprehensive_preparednessguide_developing_and_maintaining_emergency_operations_plans_2010.pdf

Hernandez, E. (2017). A look into public private partnerships for cybersecurity. Public Policy Initiative. Issue Brief: volume 6, Number 7. Penn Warton-University of Pennsylvania. https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for

I.A.C.P. International Association of Chiefs of Police. (2015). Public-private partnerships: What every chief needs to know. http://www.theiacp.org/Portals/0/documents/pdfs/IACP_PSLC_Public_Private_Partnerships_Web_080715_255p.pdf

Markle Foundation Task Force. (2006). Mobilizing information to prevent terrorism-accelerating development of a trusted information sharing environment. https://www.markle.org/publications/556-mobilizing-information-prevent-terrorism

New York Police Department. (2018). NYPD Shield. http://www.nypdshield.org/public/

Simeone, M. (2008). Integrating virtual public-private partnerships into local law enforcement for enhanced intelligence-led policing. Homeland security affairs, Proceedings of the 2008 center for homeland defense and security annual conference. https://www.hsaj.org/articles/135

U. S. Department of Homeland Security. (2016a). Critical infrastructure threat information sharing framework. https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

U. S. Department of Homeland Security. (2016b). Cybersecurity-information sharing. Retrieved from https://www.dhs.gov/topic/cybersecurity-information-sharing

U. S. Department of Homeland Security. (2017). What is critical infrastructure? https://www.dhs.gov/what-critical-infrastructure

U.S. Department of Justice. (2005). Engaging the private sector to promote homeland security: Law enforcement-private security partnership. https://www.ncjrs.gov/pdffiles1/bja/210678.pdf

U.S. Department of Justice. (2012). Federal law enforcement officers, 2008. https://www.bjs.gov/content/pub/pdf/fleo08.pdf

U.S. Department of Justice. (2013). National criminal intelligence sharing plan version 2.0. Retrieved from https://it.ojp.gov/GIST/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0

U.S. Department of Justice. (2016). National sources of law enforcement employment data. https://www.bjs.gov/content/pub/pdf/nsleed.pdf

U.S. Department of Labor. (2017). Bureau of labor statistics. Occupational Employment and Wages, May 2017. https://www.bls.gov/oes/current/oes339032.htm

U.S. Government Accountability Office. (2006). Critical Infrastructure Protection: https://www.gao.gov/products/GAO-07-39. Last accessed 5 Dec 2017.

Further Reading

Busch, N. E., & Givens, A. D. (2013). Achieving resilience in disaster management: The role of public-private partnerships. *Journal of Strategic Security, 6*(2), 1–19. https://doi.org/10.5038/1944-0472.6.2.1 Available at: http://scholarcommons.usf.edu/jss/vol6/iss2/1.

I.A.C.P. International Association of Chiefs of Police. (2004). Private security/Public policing-building private security/Public policing partnerships to prevent and respond to terrorism and public disorder. http://www.theiacp.org/Portals/0/pdfs/Publications/ACFAB5D.pdf

Simeone, M. (2008). Integrating virtual public-private partnerships into local law enforcement for enhanced intelligence-led policing. Homeland security affairs, Proceedings of the 2008 center for homeland defense and security annual conference. https://www.hsaj.org/articles/135

U. S. Department of Homeland Security. (2016). Critical infrastructure threat information sharing framework. https://www.dhs.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf

Public-Private Partnerships: Training and Coordination in Disasters

Darien A. Williams[1] and Amanda W. Martin[2]
[1]Massachusetts Institute of Technology, Cambridge, MA, USA
[2]University of North Carolina, Chapel Hill, NC, USA

Keywords

Public-private partnership · Disaster management · Disaster recovery · Disaster response · Private sector coordination

Definition

A public-private partnership (P3) is an organizational arrangement that can vary widely across contexts, particularly in disaster. According to The National Council for Public-Private Partnerships (NCPPP), as well as the US Government Accountability Office (GAO), a public-private partnership can be defined as "a contractual arrangement . . . between public and private sector partners" (GAO 1999). This is a typical definition, but in disaster contexts, public-private partnerships are not always contractual. P3s can be thought of as cross-sectoral coalitions that serve particular disaster-related needs that are not met effectively by any single sector. Involved partners can include entities from the public, private, or the nonprofit sector. North America, Asia, the Pacific, and Africa have witnessed a resurgent interest in P3s of all varieties in the last decade. Interest in this type of organization has been mixed across Europe and South America.

Introduction

Partnerships can be seen as spaces for merging motivations and values from entities in different sectors. In the public sector (and nonprofit sector to some degree), motivations for partnerships include realizing social goals, minimizing risk, democratizing a decision-making process, legislating, regulating, and navigating different authorities and political interests. Local public agencies can also be motivated by the perception of current or future lack of funding or support from higher levels of government. Private sector interests and motivations include achieving returns on investment, finding alternatives to other risky arrangements, changing market considerations, and realizing larger corporate goals (Reijniers 1994). Partnership allows interests to be coupled in pursuit of a shared goal.

Disaster public-private partnerships operate in all phases of the disaster cycle: hazard mitigation, disaster preparedness, response, and recovery. Mitigation operations are when organizations work to proactively decrease hazard exposure and vulnerability prior to a disaster event. Preparedness is the phase in which actors mobilize their "capacities and knowledge [to] anticipate and respond effectively to the impact of likely, imminent or current hazard events or conditions" (UN 2008). Preparedness activities can range from hours to years prior to a disaster event. Disaster response is the phase during and immediately following an event, in which immediate damage is assessed, prioritized, and reactive

projects are implemented (Zibulewsky 2001). Disaster response is, by nature, short-term, taking place hours, days, and sometimes weeks following an event. Disaster recovery-oriented partnerships operate in months or years following an event. These partnerships task themselves with the "process of restoring, rebuilding, and reshaping the physical, social, economic, and natural environment" (Smith et al. 2017). Partnerships may focus on a particular phase of disaster, which directs the types of projects they choose to prioritize.

Entities of all types and across all sectors can engage in public-private partnerships. These include but are not limited to governments, financial institutions, insurance firms, large and small businesses, educational institutions, faith-based organizations, professional associations, media, special districts and regional planning organizations, foundations, nonprofits, emergent groups, and individuals (Smith 2012). Some entities are bound by fewer laws, norms, and standard operating procedures than others. These more flexible organizations, such as professional associations, planning groups, and nonprofits, may naturally generate more opportunities for facilitating public-private communication and collaboration across all levels and sectors of organization (Smith 2012). Such groups may have the capacity to liaise between local residents and higher-level public and private entities. If mutually agreed upon, communication and collaboration can eventually take the form of a public-private partnership.

Leadership and Coordination

P3s often kick off through the efforts of a well-connected champion, usually an individual in a leadership position wishing to use resources towards an activity outside of what their organization typically engages in. P3 champions can be motivated to mobilize support for a partnership after perceiving a lack of funding or coordination support from federal or state governments (Chandra and Acosta 2009). Champions provide formal and informal leadership, as well as motivated partners to assume leadership roles at different levels of the organization (Simo and Bies 2007). Conversely, relying heavily on a partnership champion can leave the organization vulnerable to dissolving if the leading individual changes roles or organizations. Some partnerships attempt to address this challenge by a codifying partnership ambassador role, hiring designated partnership staff, and appointing supporting leadership roles (SDRP 2018).

After initial kickoff, P3s usually have at least two phases of planning their operations: milestone and activity planning (Reijniers 1994). Setting milestones involves visioning and mission-setting. Activity planning involves developing programs and projects to meet goals connected to the mission statement. Clearly defined geographic, organizational, and temporal scales enable the partnership to better orient its activities to unmet needs in communities or agencies that are managing the process of disaster mitigation, preparedness, response, or recovery. In some cases, while large, national-level organizations have aided short-term community recovery, long-term needs were met by smaller, locally led organizations who anticipate a drop-off of recovery support by groups and partnerships that lack long-term investment in the target community (Simo and Bies 2007). In these cases, conflict and effort duplication were managed or avoided through clearly articulated goals and well-defined scales of operation (Simo and Bies 2007). Partnerships keep on track by maintaining systems of project monitoring and progress reporting for partners, funding organizations, and/or communities they serve (Reijniers 1994).

Partnership Typology

Public-private partnership coordination can take a variety of forms, depending on the scale of organization, entities engaged, finance structures, shared goals, and phase of disaster. P3s can be arranged in reconstruction partnerships, partnerships for learning and information sharing, partnerships for planning and policy, as well as

partnerships for resource distribution (Chen et al. 2013; SDRP 2018).

Reconstruction partnerships are typically engineering and construction firms develop relationships with government agencies to inform infrastructure needs before, during, and following disaster events. Often, these arrangements span the spectrum of formality, with many starting as informal or pro bono before being codified through task force meetings and eventual organization formation. Others start contractually and carry on through later phases of disaster (SDRP 2018).

Partnerships for learning and information sharing tend to be less contractual than reconstruction partnerships. These organizations primarily aim to assist communication between government actors and private entities (including businesses, nonprofits, residents, universities, and civic organizations). Information-sharing partnerships sometimes have very specific intentions regarding the direction of information flow. Some primarily operate from the "ground up," or sharing information from a variety of actors at the local level directed to actors at central local, regional, national, and international levels of organization. Other partnerships may be more focused on information dissemination, providing a channel to communicate official information from government or corporate sources to members of a community or region. Many information-sharing P3s manage information traveling in both directions, with specific goals or projects attached to each process.

Finally, some partnerships focus on developing or informing public plans and policies for disaster recovery and resilience (SDRP 2018). These partnerships can create roadmaps for collective business continuity and mutual aid planning, municipal and regional recovery planning processes, or connect private sector perspectives with long-term questions and concerns of local, state, and federal policymakers (SDRP 2018). Planning and policy partnerships can be distinguished from learning and information sharing by their chosen time scale. Often selected timescales range from years to decades following a major event. Sometimes such partnerships are proactive and develop pre-disaster recovery plans for activation following a disaster event. Others form following an event to draft disaster recovery plans for similar time scales or engage in short-term policy changes such as building code modifications (elevation, proximity to hazards), construction standards, and re-zoning (Rotimi et al. 2011). Learning and information-sharing tend to prioritize present conditions, where planning and policy partnerships operate future-oriented.

Partnerships may be created for the explicit purpose of distributing material resources to residents prior to an event or survivors following the disaster. These P3s tend to be event-specific, with collaborations between major retailers with supply chain network infrastructure and expertise deemed suitable for disaster-related supply distribution (Stewart et al. 2009; Kapucu et al. 2010). Such partnerships are usually small and involve senior business leaders and government officials, with a goal of delivering a specified good or set of goods to target communities.

Disaster P3s can begin as loosely coordinated, untrained coalitions of concerned professionals who see common interest and mutual benefit in collaboration following a disaster event. While some types of partnerships are more active in certain phases of disaster than others, all types may have operations throughout the entire disaster cycle. Often partnerships organize and register as a 501(c)(3) or other nongovernmental organization in order to secure access to the widest range of funding sources to sustain partnership projects.

There are several ways in which becoming a 501(c)(3) helps disaster-related partnerships. In the United States, partnerships operating as 501(c)(3)s are excluded from taxes, and this status is required in order to apply for grants offered by local, state, and federal government as well as private foundations and other funding agencies. These grants may require that applicants commit other resources toward a project to generate greater buy-in by the applicant. Partnerships often are well suited for the collaboration required

to find matching funds or in-kind support for projects that support common goals. In addition, the financial and administrative capacities required of a 501(c)(3)s help partnerships maintain operations beyond the initial triggering disaster event (SDRP 2018). The work to draft a mission statement, often associated with official nongovernmental organization status, guides projects and interventions the organization chooses to engage in. Mission statements become an asset for preserving institutional memory about partnership intent, reducing the potential for coordination conflict down the line (SDRP 2018).

Training

Training is a major activity of P3s. Some partnerships run drills or facilitate workshops that train their own members, private sector leaders, or government actors in how to effectively work with each other. These efforts often involve expert facilitators guiding a discrete numbers of predetermined participants and audiences. Other partnership training efforts involve entire target communities, including residents and business leaders. These training processes usually intended to inform community trainees on programs, resources, and ways to safely act and operate during different phases of disaster. These training efforts may involve a wide range of actors, needs, and levels of expertise. Many of these larger partnership training efforts rely on the support of volunteer labor, which can be challenging to find in abundance during "blue skies" (or non-disaster operation), but difficult to manage alongside emergent needs following a disaster event (Quero 2012). If the partnership has an operating budget, they may hire part- or full-time coordinating staff to facilitate outreach and training programming (SDRP 2018).

Many partnerships engage all partners in regular outreach and programming in order to keep relevant entities organizationally on the same page with clear, rehearsed, understood channels of communication. Community- and resident-facing partnerships may also develop separate strategies for regularly engaging the populations they serve.

Engagement with partners or the public can take the form of a monthly meeting, volunteer days, disaster drills, workshops, shadowing, and workplace visits (SDRP 2018). Regular points of engagement sustain interest and motivation required for different types of organizations to effectively coordinate in later, more constrained contexts. Engagement has the added benefit of ensuring institutional knowledge and working organizational relationships are maintained, offering familiarity that serves the partnership's needs during a disaster event when all organizations lack time and capacity to form many new relationships and working dynamics.

Conclusion

Public-private partnerships have emerged as a way to incorporate the skills, resources, and knowledge of wider segments of the community and economy in overall disaster preparedness, mitigation, response, and recovery. P3 organizations range from disaster- and region-specific initiatives of local players to standalone organizations with national and international missions. They are often convened and strengthened by very active champions with personal and professional connections that motivate skilled and resourced partners. As climate disaster events become increasingly challenging to predict, and as human settlements expand into geographies previously thought too hazardous, motivated organizations will likely be required to think through creative strategies for funding and implementing disaster-related projects and interventions.

Cross-References

- ▶ Emergency Management: Best Practices
- ▶ Emergency Management: Crisis Management and Response
- ▶ Emergency Management: Preparedness and Planning
- ▶ Emergency Management: Recovery

References

Chandra, A., & Acosta, J. D. (2009). The role of non-governmental organizations in long-term human recovery after disaster: Reflections from Louisiana four years after Hurricane Katrina. Rand Corporation.

Chen, J., Chen, T. H. Y., Vertinsky, I., Yumagulova, L., & Park, C. (2013). Public–private partnerships for the development of disaster resilient communities. *Journal of Contingencies and Crisis Management, 21*(3), 130–143.

GAO. (1999). *Public-private partnerships*. Retrieved from https://www.gao.gov/special.pubs/Gg99071.pdf

Kapucu, N., Arslan, T., & Demiroz, F. (2010). Collaborative emergency management and national emergency management network. *Disaster Prevention and Management: An International Journal, 19*(4), 452–468. https://doi.org/10.1108/09653561011 070376.

Martin, A., Williams, D., Southeast Disaster Recovery Partnership (SDRP). (2018). *For the long Haul: Public-private partnerships for long-term disaster recovery.* Retrieved from http://secoora.org/wp-content/uploads/2018/06/Partnerships_for_Disaster_Recovery.pdf

Quero, R. A. (2012). Reframing coordination challenges for public-private partnerships in disaster preparedness. *Procedia – Social and Behavioral Sciences, 57*, 440–447. https://doi.org/10.1016/j.sbspro.2012.0 9.1209.

Reijniers, J. (1994). Organization of public-private partnership projects. *International Journal of Project Management, 12*(3), 137–142. https://doi.org/10.1016/0263-7863(94)90028-0.

Rotimi, J. O., Wilkinson, S., & Myburgh, D. (2011). Legislation for effective post-disaster reconstruction: Cases from New Zealand. *Post-Disaster Reconstruction of the Built Environment*, 151–174. https://doi.org/10.1002/9781444344943.ch9.

Simo, G., & Bies, A. L. (2007). The role of nonprofits in disaster response: An expanded model of cross-sector collaboration. *Public Administration Review, 67*, 125–142. https://doi.org/10.1111/j.1540-6210.2007.00 821.x.

Smith, G. (2012). *Planning for post-disaster recovery: A review of the United States disaster assistance framework*. Washington, DC: Island Press.

Smith, G., Martin, A., & Wenger, D. E. (2017). Disaster recovery in an era of climate change: The unrealized promise of institutional resilience. In *Handbook of disaster research* (pp. 595–619). https://doi.org/10.1007/978-3-319-63254-4_28.

Stewart, G. T., Kolluru, R., & Smith, M. (2009). Leveraging public-private partnerships to improve community resilience in times of disaster. *International Journal of Physical Distribution & Logistics Management, 39*(5), 343–364. https://doi.org/10.1108/09600030910 973724.

United Nations (UN). (2008). Hyogo framework for action – Disaster preparedness for effective response. Retrieved from United Nations website: https://www.unisdr.org/files/2909_Disasterpreparednessforeffectiveresponse.pdf

Zibulewsky, J. (2001). Defining disaster: The emergency department perspective. *Baylor University Medical Center Proceedings, 14*(2), 144–149. https://doi.org/10.1080/08998280.2001.11927751.

Further Reading

Chen, J., Chen, T. H. Y., Vertinsky, I., Yumagulova, L., & Park, C. (2013). Public–private partnerships for the development of disaster resilient communities. *Journal of contingencies and crisis management, 21*(3), 130–143.

Southeast Disaster Recovery Partnership (SDRP). (2018). *For the long Haul: Public-private partnerships for long-term disaster recovery*. Retrieved from http://secoora.org/wp-content/uploads/2018/06/Partnerships_for_Disaster_Recovery.pdf

Stewart, G. T., Kolluru, R., & Smith, M. (2009). Leveraging public-private partnerships to improve community resilience in times of disaster. *International Journal of Physical Distribution & Logistics Management, 39*(5), 343–364. https://doi.org/10.1108/09600030910 973724.

R

Rail (Train) Security

Veronica Strandh
Department of Political Science,
Umeå University, Umeå, Sweden

Keywords
Trains · Rail bound traffic · Security · Terrorism · Emergency management response

Definition

Rail security: rules, procedures, and processes to *protect* the railway system and efforts to *mitigate, respond*, and *recover* from attacks targeting rail bound traffic.

Introduction

Modern society is characterized by its interconnectedness, i.e., important critical dependencies exist which are essential to the maintenance of daily life. Rail bound traffic is a fundamental part of the so-called critical infrastructure of a society. Rail bound traffic, which is both passenger traffic, freight traffic, subway systems and its surrounding infrastructure, is an integral part of the overall transportation system. Trains are not only essential for the country's urban infrastructure but also for connecting people across geographic areas. Railway systems are also designed for accessibility and efficiency. However, critical infrastructure systems, including railway systems, also appear vulnerable to different acts of terrorism. A major current concern is that railway systems will be affected by cyberattacks. The terrorist events in Madrid in 2004 (almost 200 people were killed and nearly 2000 injured) and in London in 2005 (56 people were killed and 700 injured) are two examples of large-scale attacks which demonstrated the enormous consequences of a terrorist attack against rail bound traffic, not only in terms of human suffering but also in terms of major disruptions in vital societal functions. Attacks have also repeatedly targeted Russian railway and subway systems, including events in 2007, 2009, 2010, 2013, and 2017. Another example is the Brussels bombings in 2016, in which a bomb exploded on a train at the Maalbeek metro station. There are also several documented examples of thwarted attacks, and rail bound traffic is often mentioned in the media as a potential target for acts of violence. For example, there have been several reports on thwarted attacks in the United States, and New York's subway system has been identified as a main target.

In light of these major attacks on rail bound traffic, it is rather surprising that previous research has devoted extensive attention to terrorism targeting *other* forms of public transportation, including aviation and buses. Despite its inherent vulnerabilities, less attention has been paid to rail bound traffic (Strandh 2015a).

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

A Vulnerable Rail Bound Traffic

A general development in present-day terrorism is an identifiable shift toward more indiscriminate killings. Recent attacks targeting the public transportation sector have involved trucks, cars, and mopeds as weapons. As the examples already mentioned show, the rail bound traffic appears extremely vulnerable to attacks, and scholars (Jenkins 2001) even argue that, in the eyes of terrorists, it seems that rail bound traffic is becoming a "perfect" target to attack when the goal is to cause mass-casualty events. The question is then, why is the rail bound traffic so difficult to protect and what makes it a "perfect target" for terrorists?

1. *The open character.* One of the most distinguishing features of a rail bound system is its openness. There are few security measures on railway systems due to the need for easy passenger access and the railway system's wide geographical coverage. Passenger profiling, metal detectors, and patrolling police, all of which have become part of the landscape at airports, cannot be applied to rail bound traffic in the same way
2. *The possibility of anonymity.* It is, for instance, possible for the perpetrator to leave a backpack containing explosives on a train and then exit the train at the next station with several escape routes
3. *Large number of casualties.* Trains and railway stations mean large numbers of passengers in confined spaces, and this is attractive to terrorists who want their attacks to produce a large number of casualties
4. *Critical dependencies.* Attacks on railway systems cause enormous human suffering, but they can also cause major disruptions in vital societal functions. The risk for long-lasting cascading effects due to the disruption or destruction of a critically important infrastructure such as rail bound traffic is significant, and it becomes crucial to protect this sector against long periods of breakdown.

If terrorists seek to cause significant human suffering and cause major societal infrastructure consequences, rail bound traffic will most likely remain a target for acts of terrorism. The combination of the different inherent vulnerabilities associated with this transportation sector strongly indicates that the threat of terrorism can never be entirely eliminated. Hence, many researchers seem to agree that current available security and mitigation efforts cannot *completely* prevent attacks from occurring (Jenkins 2001, 2012; Waugh 2004; Strandh 2015a).

Attacks on Rail Bound Traffic: What Are the Main Characteristics?

First of all, terrorist attacks targeting trains or subway systems are nothing new. History provides us with plenty of evidence that trains, stations, and railway tracks have been targets of sabotage and attacks for a long time. However, like other means of transportation, rail bound traffic has now become a theater of operation for terrorists whose goal is to cause mass-casualty events (Jenkins 2001).

The phenomenon of terrorism targeting rail bound traffic is a *global* concern. Attacks take place in different parts of the world, and have done so since 1970, when terrorist attacks began to be registered systematically in research databases (Strandh 2015a). Using the Global Terrorism Database (GTD at the University of Maryland), Strandberg (2013, see also Strandh 2015a) analyzes attacks against rail bound traffic during a 40-year period. The results show that an overwhelming majority of the attacks since 1970 (1122 attacks in total) can be categorized as small ones that resulted in few casualties and limited infrastructure damage. This finding supports previous research on terrorism, which, in contrast to the widespread perception of terrorism as something that is always lethal, demonstrates that most terrorist attacks do not produce a large number of casualties. These minor attacks on rail bound traffic, with few casualties, are carried out by many different kinds of terrorist groups, and they are geographically diverse and tend to target different parts of the railway infrastructure. The analysis (Strandberg 2013; Strandh 2015a) also shows

another pattern, a rather recent development in which we can identify an increase in major, high-profile cases: nearly half of the 20 largest-scale attacks on railway traffic occurred after 2001. These attacks use a modus operandi designed to create as much destruction and fear as possible, including coordinated bombings resulting in multiple incident sites and attacks during rush hours. These high-profile cases result in complicated mass-casualty situations with an increasingly high number of casualties. In particular, the number of injured in the attacks has increased over the years. As mentioned earlier, the Madrid bombings, the London bombings, and the Brussel bombings are a few examples of this development.

Returning to the inherent vulnerabilities associated with rail bound traffic, the analysis over attacks since the 1970s shows that terrorists tend to target *different* parts of the railway sector. Forty-six percent of the attacks were targeting parked or passing trains. Yet, 22% of all attacks have targeted stations, and 17% have focused on railway tracks. Nine percent of the attacks were directed against railway support equipment, while freight trains were the target in 6% of the attacks. This confirms the picture of the railway sector as extremely difficult to protect and poses security dilemmas. For example, increased security measures at train or metro stations are considered an important security measure, but as the overview of attacks shows, 17% percent of all attacks target the actual railway tracks, and those attacks cannot be prevented by security measures at the stations (Strandberg 2013).

In terms of modus operandi, previous research (Frykberg 2002) contends that bombing is the most common method of attack. This is true also for attacks targeting trains. Bombs have been used in 78% of all railway bound cases. Armed assault accounted for 13%, and incendiary attacks were reported in 5% of all cases (Strandberg 2013).

The world has unfortunately experienced a number of high-profile terrorist events, and cases like September 11 tend to signal that terrorist strikes rely on highly sophisticated weapons, but the majority of attacks actually involve explosives or firearms. This is, as stated, also an accurate description of attacks on rail bound traffic. Bombs are relatively easy and inexpensive to construct, and it is widely known that terrorists use the Internet as a way to share detailed instructions about how to make bombs. A recent development is also that terrorist groups call for lone wolf perpetrators to use simple, improvised weaponry.

Another central question when trying to understand the characteristics of terrorism against rail bound traffic is the following: Who is behind the different attacks? Again, looking at the 40-year period, it can be concluded that there is a broad spectrum of terrorist groups behind the events. The Global Terrorism Database lists 150 different terrorist organizations that are responsible for attacks against this particular transportation sector. From a security perspective, it becomes interesting to note that what stands out is the high percentage of unknown perpetrators. In 51% of all attacks, there is no known perpetrator, and this once again confirms the picture of the rail bound traffic as problematic to protect and that the perpetrators can remain anonymous (Strandberg 2013).

The most recent data from the Global Terrorism Database reveals that there have been 25 large-scale attacks targeting rail bound traffic during the last 5 years (2013–2017). These attacks are events with more than ten causalities. There is a wide geographic distribution of the most recent large-scale attacks, including countries such as Russia, India, Thailand, Bangladesh, China, Egypt, and Great Britain. Pakistan stands out as the single most exposed country; 11 of the 25 large-scale attacks took place in Pakistan. Europe, which was hard hit by the London bombings in 2005 and the Madrid bombings in 2004, has not suffered any more attacks on the same scale. The attacks that have taken place since 2013 follow the same pattern as previous attacks in that regard that the different parts of the railway system are targeted. Bombings directed at passenger trains are the most frequent modus operandi, but there are also examples of armed assaults targeting train stations or sabotage of railway tracks. The phenomenon of suicide attacks is often discussed when analyzing present forms of

terrorism. One can note that 3 of the 25 most recent large-scale attacks were suicide events.

Hence, the pattern continues; a large majority of the attacks targeting rail bound traffic consists of smaller events with limited consequences, and they do not make headline news. Yet, the large-scale attacks do occur but not as frequent as the smaller ones. This causes a policy dilemma; should resources be allocated for investing in preparedness for such "low probability-high consequences events"? It is seldom that major large-scale cases occur, but if they do, their consequences will be enormous.

Rail Security and Emergency Management

As mentioned, high-profile terrorist events against trains are a rather recent development. If this trend continues, one can anticipate the need for highly complicated emergency management response efforts. Particular emphasis should be given to evacuation, search and rescue efforts, and medical care, because there are opportunities to save lives even after a terrorist attack. There is no universal solution to how to organize emergency management in the context of terrorism targeting rail bound traffic; however, there are some recurring critical points in the emergency management processes following the attacks.

A comparative analysis (Strandh 2015b) of attacks targeting Tokyo's subway system in 1995 and the bombings on commuter rail systems in Madrid in 2004, London in 2005, and Mumbai in 2006 illustrates some recurring challenges in the response. All cases showed how the response to a mass-casualty event is highly demanding in terms of (1) performing triage, (2) carrying out lifesaving measures, and (3) coordinating initial resources under circumstances of significant uncertainty and time pressure.

Important, however, is the realization that a terrorism-induced crisis also implies *additional* challenges. The large-scale events in Tokyo, Madrid, London, and Mumbai are examples of how these additional prehospital challenges can play out. (1) If a multi-site terrorist attack takes place (for instance, simultaneously bombings targeting a passenger train and a subway station), it will create several incident sites, which tends to make it extremely difficult for first responders to develop an understanding of the situation. As a consequence, it becomes difficult to grasp the extent and nature of the attack and to distribute resources and establish command structures at several parallel sites. (2) In a terrorism-induced event, scene safety emerges as particularly precarious. Secondary devices and exposure to dangerous substances are examples of the risks facing both emergency rescue personnel and victims. This also affects how assembly points and hospital tents can (or cannot) be established. (3) Security concerns call for rapid scene clearance, which, in turn, poses additional challenges because it leads to significant and rapid surge at hospitals. Evacuation and rapid scene clearance can be particularly challenging when trains are involved. The incident site, might, for instance, be located underground in a subway system or inside a railway tunnel. (4) The modus operandi of different terrorist groups results in specific injury patterns. The four cases mentioned here, Tokyo, Madrid, London, and Mumbai, were attacks involving chemical substances or bomb explosions. According to previous research (Frykberg 2002; Gómez et al. 2007), such injury patterns cause additional concerns. Persons injured in bomb explosions or shootings tend to bleed to death; thus, rapid action is needed. It is reasonable to assume that such injury patterns are far removed from what most medical services encounter on a daily basis. Instead, they are more often associated with injury patterns commonly found in war zones.

Rail Bound Traffic Actors: Fragmentation and New Roles

How to improve rail security and secure rail bound traffic from acts of terrorism has become a growing concern, and as pointed out several times, this particular transportation sector is extremely challenging to secure from antagonistic acts. This is due to its inherent vulnerabilities such as it openness. However, another aspect of this discussion relates to institutional aspects. Hence,

what characterizes this transportation sector in many countries is its *fragmentation.* This observation indicates that a paradox seems to exist. Thus, as stated, our society is becoming increasingly interconnected, and there are important dependencies in critical infrastructures, rail bound traffic included. While this seems to lead to the conclusion that critical infrastructures require a unified management, what we actually observe is increased organizational fragmentation (Strandh 2017).

Rail bound traffic is largely privately owned and consists of a multitude of different actors. The railway environment in many countries can be described as a patchwork of actors. Some actors are responsible for passenger traffic and others for freight rail. Some companies are domestic, while other operators are partly owned or wholly owned by international actors. There might be additional actors responsible for infrastructure, maintenance, and real estate. In addition, different government authorities are usually responsible for different questions relating to transportation and railway. Without a doubt, the often high number of participating actors and increased fragmentation raises questions about the possible implications of this development for security and emergency management. One could argue that more actors provide an opportunity to enhance security on the railroad in that sense that more actors are working dedicated to improve safety and security. However, one could also argue that an increased fragmentation runs the risk of creating vulnerability from a security and emergency management perspective. The organizational fragmentation is manifest, for instance, in unclear responsibilities, lack of overview over a multitude of actors, and an absence of a unified approach about how to mitigate and prepare for different forms of security challenges (Strandh 2017).

It can be noted that security work and terrorist attacks are foremost associated with intelligence, law enforcement, fire service, and emergency medical services. However, rail bound traffic actors increasingly, through private-public partnerships, assumed to take an active role when societal crises occur. An identified challenge is the railway sector's unfamiliarity with working in uncertain crisis settings, even though they are assumed to operate in the more peripheral parts of a response following a terrorist attack. Their role adheres foremost to avoiding a transportation breakdown and alternatively to resuming operation as soon as possible or communication to affected and stranded passengers. However, they nevertheless need to know their mandate and resources and have an understanding of the procedures that goes beyond daily operation. The question of whether an increased fragmentation of the sector improves or hinders their capacity to participate in such a process will continue to be discussed.

Efforts to Increase Security

There is no universal solution to the question of how to best enhance rail security and protect it from antagonistic acts. The response of security agencies and emergency management authorities have also varied around the world. A traditional approach is to focus on technical aspects of security or physical structures in prevention and preparedness. It is, for instance, widely known that London, which suffered from the bombings in 2005, use a vast network of CCTV cameras for surveillance. Such efforts are combined with extensive police patrols and intelligence work in order to thwart attacks. Even though security measures such as passenger profiling and metal detectors are not applied to the same extent as at airports, there are examples of increased security procedures at railway stations. For example, both Delhi and Moscow have comprehensive security procedures, searching for explosives and other weapons. However, a common discussion revolves around how to detect potential terror threats without compromising commuters' privacy.

Given the fact that rail traffic is so hard to protect, some researchers argue that protective security measures should focus on reducing the probability of an attack and *limiting* the damage caused by the attacks rather than focusing on eliminating *all* threats of attacks. Accordingly, so-called protective design is frequently discussed. Increased collaboration with architects

and designers in order to improve station design is one example. Another example is to develop a design of railway station which enables and improves evacuation flows in case of emergency situations. Also efforts to mitigate the effects of fires and explosions on trains and at stations are frequently being discussed (Strandh 2017; Holgersson 2016).

Another development shows that it is increasingly common for railway companies and security agencies to trust ordinary railway employees with the task to look for and report suspicious objects and individuals. In some countries, it is also common that ordinary passengers or visitors at a central station are encouraged to report suspicious behavior and activity.

Conclusion

In conclusion, railway systems can be a unique security challenge. One of the most distinguishing features of the rail bound system is its openness and thus its vulnerability. Trains, subways, stations, and tracks become attractive targets for terrorists for a number of reasons: the open character of the system, the possibility of anonymity, the large number of potential casualties, and the potential to disrupt critical infrastructure. A major attack on rail bound traffic can cause a highly complex mass-casualty situation which is demanding in terms of performing triage, carrying out lifesaving measures, and coordinating initial resources. Furthermore, it can be concluded that a terrorism-induced crisis also implies additional response challenges including several incident sites, scene safety for victims and rescue personnel, rapid scene clearance, and unique injury patterns. Moreover, rail security efforts are also closely related to the institutional rail environment, an environment which in many countries can be described as a patchwork of actors. An increased institutional fragmentation can create new vulnerabilities, for instance, unclear responsibilities, lack of overview over a multitude of actors, and an absence of a unified approach about how to mitigate and prepare for different forms of security challenges. Much remains to be done about rail security; however, the question of how to secure this transportation sector from acts of terrorism and other acts of violence keeps being discussed, and we can expect new rail security efforts in the future. Importantly, however, such security proposals must be realistic and suited for the unique character of the railway system.

Cross-References

- ▶ Border Security
- ▶ Criminals: Active Shooters
- ▶ Criminals: Terrorists
- ▶ Critical Infrastructure: Transportation Systems

References

Frykberg, E. (2002). Medical management of disasters and mass casualties from terrorist bombings: How can we cope? *The Journal of Trauma, 53*(2), 201–212.

Gómez, A., Dominguez, C., Pedrueza, C., Calvente, R., Lillo, V., & Canas, J. (2007). Management and analysis of out-of-hospital health-related responses to simultaneous railway explosions in Madrid, Spain. *European Journal of Emergency Medicine, 14*(5), 247–255.

Holgersson, A. (2016). *Preparedness for mass-casualty attacks on public transportation*. Dissertation, Department of Surgical and Perioperative Sciences, Umeå University.

Jenkins, B. (2001). *Protecting public surface transportation against terrorism and serious crime: An executive overview* (Report FHWA/CA/OR-2001-29). San Jose: Mineta Transportation Institute.

Jenkins, B. (2012). The transportation threat to surface transportation: The challenges of securing public places. In D. Kamien (Ed.), *The McGraw-Hill homeland security handbook: Strategic guidance for a coordinated approach to effective security and emergency management* (pp. 21–31). New York: McGraw-Hill.

Strandberg, V. (2013). Rail bound traffic – A prime target for contemporary terrorist attacks? *Journal of Transport Security, 6*(3), 271–286.

Strandh, V. (2015a). *Responding to terrorist attacks on rail bound traffic challenges for inter-organizational collaboration.* Dissertation, Department of Political Science & Department of Surgical and Perioperative Sciences, Umeå University.

Strandh, V. (2015b). Preparing and responding to mass casualty terrorist attacks: A comparative analysis of four terrorist attacks targeting rail bound traffic. *International Journal of Emergency Management, 11*(3), 262–281.

Strandh, V. (2017). Exploring vulnerabilities in preparedness: Rail bound traffic and terrorist attacks. *Journal of Transportation Security, 10*(3–4), 45–62.
Waugh, W. (2004). Securing mass transit: A challenge for homeland security. *Review of Policy Research, 21*(3), 307–316.

Further Reading

Johnston, V.R., & Plant, J.F. (2008). Rail security after 9/11: Toward effective collaborative regulation. Public Works Management & Policy, 13(1), 12–21.
Hakim, S., Albert, G., & Shiftan, Y. (2016). Securing transportation systems. Hoboken, NJ: John Wiley & Sons.
Sasnett, Q (2017). Rail travel in the United States: Metropolitan Washington DC rail travelers' perception of security and the concepts of privacy and liberty. ProQuest Dissertation Publishing, Northcentral University. 10642893. Accessed at: https://search-proquest-com.ez.lib.jjay.cuny.edu/docview/1973067071/?pq-origsite=primo (7/3/19).

Residential Security: Gated Communities

Trevor A. Smith[1] and Christopher A. D. Charles[2]
[1]University of the West Indies, Mona, Jamaica
[2]Department of Government, University of the West Indies, Mona, Jamaica

Keywords
Gated communities · Residential security · Non-gated communities · Safety · Segregation · Neighborhood watch · Service workers

Definition

A gated community is a residential complex with its boundaries enclosed by walls, fences, and embankments and has restricted access and other security systems to allow for the protection, safety, and comfort of the residents.

Introduction

The chapter examines residential security within the context of gated communities. Residential security involves the protection of people and their properties from the risk of burglary, home invasion, threats, disturbances, and other vulnerabilities. Thus, residential security is the type of protection that is offered to gated communities as it provides estate protection and other security solutions for the household.

The gated community has become an international trend over the last few decades. It consists of homes, green spaces, security guardhouses, electronic gates, controlled entrance, surveillance systems and enclosed by walls, fences, and embankments. This physical and symbolic separation of houses from the outside neighborhood is not a new phenomenon and many early examples, such as the Lincoln's Inn Field in 1735 and the Golden Square in 1750, date back to Western Europe of the eighteenth century (Porcu 2013).

At the entrance to the community, there is usually a guard booth operated by private security personnel and/or an automatic gate with remote control card access that is operated by residents. Visitor access to these premises is directed by the security guard in consultation with the resident, who is being visited, or by the resident him/herself who gives access through the remote gate. These properties are also equipped with pedestrian gates to allow convenience to authorized personnel to walk in and out of the premises. Speed bumps are also installed in these premises to regulate the speed of vehicular traffic thus making it safer for children to play within the grounds and for residents to more freely utilize the roadways.

These walled communities can be found in both rural and urban areas and are spatially organized to provide a picturesque view of houses, small streets, and green spaces. Many of these communities are equipped with parks, fitness centers, shopping complexes, meeting rooms, recreational facilities, and other common areas. Most of these properties are privately owned, making it legal to deny public access to the properties. However, some of these occupants are renters. The privatization of public spaces such as shopping malls and recreational parks within gated communities are facilitated by governments thereby limiting the use of these spaces to the wider public and giving the residents control over the complex.

In these communities, there are individual owners of the units while other parts of the property, such as clubhouses, swimming pools, and shared areas are owned in common by the residents. These communities are managed by associations which are comprised of residents who are elected as officers by the wider body of residents for the primary purpose of managing the affairs of the residential complex. The residents are required to conform with the bylaws of the association which stipulate the code of conduct and responsibilities of these householders. These bylaws would usually address issues such as usage of grounds, common areas, and facilities. A monthly association fee agreed by the owners is charged to the households by the association for securing the property and operating and maintaining common areas. These fees are often seen as double taxation by residents as they cover services such as trash collection which is already covered in taxes paid to local authorities (Lang and Danielsen 1997). The association sometimes takes some property owners to court to recover monthly fees owed. The law in some countries allows the association to legally force delinquent owners to sell their properties to recover substantial sums of monthly fees owed.

Motivation for Living in Gated Communities

Gated communities can be divided into three types. These are *security communities* where the focus is on the protection from crime, *prestige communities* where the orientation is on social status, and *lifestyle communities* where the core motivation is the availability of amenities for the convenience of the residents (Blakely and Snyder 1997). People move into these communities because of the fear of crime, fear of others, general safety, protecting property values, preservation of orderliness, and search for community, retiree needs, and regeneration of one's childhood neighborhood. Residents generally deem gated communities to be safer than the alternatives, regardless of what their primary motivation is for living in a gated community (Sullivan 2006).

Safety and Crime in Gated Versus Non-gated Communities

Living in a gated community allows for a trade-off between freedom and safety, i.e., freedom is curtailed due to the restrictions of the community while safety is promised with the use of manpower, barriers, and technology. People buy into gated communities to protect their families and properties from the risk of crime along with the urban unrest and instability that characterize modern society. Most of the affluent gated communities are monitored by 24-h private security guards while the not so affluent may use technological devices instead of guards. Some of the less affluent communities may not even use the technology but simply rely on the physical barriers as a mere psychological symbol of protection. These security measures and barriers afforded by gated communities appear to influence the residents' perceptions and sense of safety.

Safety is also thought to be facilitated by the restriction of visitor and vehicular access to the property. Some gated communities provide residents with a bar code for their vehicles. This allows for easy and quick access to the premises. The gates open and close in a few seconds after the bar codes which are placed on the car windscreen are scanned. This restricted access will allow for less intrusion of the properties and less opportunities for criminals to commit crimes. Thus, gated communities are designed to address the pervasive need for safety. Despite this view, there is no concrete evidence to support the belief that homes in gated communities are safer than those in non-gated properties (Low 2001, 2007).

For example, a study on gated versus non-gated communities in Newport Beach, California, Unites States, found no significant difference in perceived safety and actual crime rates between gated and non-gated communities – whether these communities were situated in high- or low-income neighborhoods (Wilson-Doenges 2000). Another study found that crime levels decreased after the development of gated communities but returned to previous levels in subsequent years (Fowler and Mangione 1986). Research is also suggesting that gated communities increase the feel of safety for residents while simultaneously increase the fear of

these residents for the outside world (Sarpong 2016). There is also the issue of domestic violence that take place behind the walls of gated communities as well as the con-artist usage of telephone scamming to steal from the elderly. Gated communities cannot prevent domestic violence since it is perpetuated by residents against family members or scamming since personal telephones are the channels used to commit this crime. However, more effective management and use of guards and surveillance of gated communities can prevent certain crimes, for example, burglary and other property crimes that sometimes occur in these residential facilities. Although a recent study found that surveillance systems within gated properties have led to the reduction in crimes, the overall research findings are mixed as to whether there is lower incidents of crime in gated than non-gated communities because the nature and organization of gated housing enclaves reveals that they can only mitigate certain type of crimes (Hedayati-Marzbali et al. 2017; Jacobs and Addington 2016; Reiboldt and Vogel 2001).

Affluence, Segregation, and Social Inequity

Gated communities are indexed to levels of segregation in the metropolitan areas of the United States. Therefore, an increase in the numbers of gated communities is expected to increase the levels of segregation in the country (Denton and Massey 1998). People also buy into gated communities in search for social and ethnic homogeneity amid the heterogeneity of urban societies. This separation also provides residents with a sense of tranquility as it creates a safe distance from the urban chaos and disorder (Caldeira 2000).

These gated complexes are described as common interest communities as they are designed to attract people of similar interests. These communities are also thought to address the desire for prestige and affiliation among residents (Low 2001, 2007). The communities provide exclusive usage of service and resources and are usually high-value properties that maintain value even when house prices within surrounding neighborhoods are falling. People opt to buy properties in these complexes because of the sustained property value as well as the perceived notion of safety in the living environment which also adds to the property value.

Residential gated facilities are seen as a place to live for people who share the same social status. They are also viewed as a place for children to grow up and play with peers of the same social standing and hence being isolated from some of the vagaries and deviant behaviors of the wider society. These enclaves are criticized for creating a place of segregation and social inequity within society (Low 2001, 2007). The properties are often thought to be a status symbol with the physical barriers perceived as a basis of economic inequality between neighbors living inside and outside the communities. As such, these properties engender an inward focused community culture driven by collective self-interest and bear the social cost of isolation and not identifying with the regions outside. And even on the inside, there are issues of *social trepidation* where residents are seemingly reluctant to speak with each other, even on trivial matters such as loud noises made by residents or children playing in unauthorized areas.

Neighborhood Watch

The neighborhood watch is a crime prevention strategy that is utilized by some gated communities. This involves the participation of residents in monitoring of the neighborhood to ensure that all suspicious activities and noncompliant behaviors, both within the community and in proximity to the community, are reported to the police. This vigilance by the citizens is of utmost importance as the police will always be constraint in providing the necessary 24-h monitoring of these surroundings. These neighborhood watch groups are indicative of residents' fear despite the leveraging of a range of security assets – paid manpower, barriers, and technology.

Security and Service Workers

Gated communities interact with the surrounding areas through service workers such as gardeners, nannies, and maids who are often drawn from

nearby low-income neighborhoods. These workers play a meaningful role in protecting community properties from the perspective of securing the property investment and providing *watchman-like* services for these properties. A case in point is the zone of gated communities near Belo Horizonte in Brazil where the gardeners employed to the communities were associated with the preservation of property investments through landscaping and manicuring of lawns thus keeping up the real estate values (Chase 2008). The well-kept properties also gave the impression that people are always around the place, even if not seen, hence providing another layer of security for the gated properties. These gardeners over time become social bridges between the gated and low-income communities because they build social capital between these communities thereby making the gated communities safer.

Conclusion

The gated community residents are the privileged few that are seemingly protected from the dangerous outsiders rather than the dangerous insiders. However, this preoccupation with the safety of the gated few diminishes collective responsibility for the safety of the masses thus perpetuating inequity within society. As such, living in gated communities is seen to increase the social capital among the rich and middle class who socially interact and share amenities and perceived safety behind these gates. However, the building of social capital in this exclusive manner does not bring social benefits to the wider society, as the outside majority is excluded from the added layer of protection that is offered by these properties. Thus, gated communities can be viewed as a temporary escape from reality as the space of fear outside these gates are always expanding. In effect, the security of people can only be improved, in a real way, when social exclusion and poverty are meaningfully addressed in the wider society.

Notwithstanding the perceived societal ills that have been associated with gated communities, the residents living within the complexes continue to benefit from the security, prestige, and lifestyle that are offered by these properties and are still holding on to the psychological feel of safety that is afforded by the barriers. Property values are also thought to be better maintained with gated communities even though the evidence varies based on location.

Cross-References

▶ Residential Security: Houses and Apartments, Public and Private

References

Blakely, E. J., & Snyder, M. G. (1997). *Fortress America: Gated communities in the United States*. Washington, DC: Brookings Institution Press.

Caldeira, T. P. (2000). *City of walls: Crime, segregation, and citizenship in São Paulo*. Berkeley: University of California Press.

Chase, J. (2008). Their space: Security and service workers in a Brazilian gated community. *Geographical Review, 98*, 476–495.

Denton, N. A., & Massey, D. S. (1998). The dimensions of residential segregation. *Social Forces, 67*, 281–315.

Fowler, F. J., Jr., & Mangione, T. W. (1986). A three-pronged effort to reduce crime and fear of crime: The Hartford experiment. In D. P. Rosenbaum (Ed.), *Community crime prevention: Does it work?* (pp. 87–108). Newbury Park: Sage.

Hedayati-Marzbali, M., Maghsoodi Tilaki, M. J., & Abdullah, A. (2017). Assessing the effect of neighbourhood structure on residents' perceptions of safety in gated communities: A case study of Iran. *Safer Communities, 16*, 3–19.

Jacobs, B. A., & Addington, L. A. (2016). Gating and residential robbery. *Crime Prevention and Community Safety, 18*, 19–37.

Lang, R. E., & Danielsen, K. A. (1997). Gated communities in America: Walling out the world? *Housing Policy Debate, 8*, 867–899.

Low, S. M. (2001). The edge and the center: Gated communities and the discourse of urban fear. *American Anthropologist, 103*, 45–58.

Low, S. M. (2007). Behind bars. *The Next American City Fall, 16*, 28–31.

Porcu, M. (2013). Gated communities and control of urban space. An inventory of fixtures. *Deviance and Society, 37*, 229–247.

Reiboldt, W., & Vogel, R. E. (2001). A critical analysis of telemarketing fraud in a gated senior community. *Journal of Elder Abuse & Neglect, 13*, 21–38.

Sarpong, S. (2016). Building bridges or gates? Gated communities' escape from reality. *International Journal of Social Economics, 44*, 1584–1596.
Sullivan, D. M. (2006). Behind the gates: Life, security, and the pursuit of happiness in fortress America. *Population, Communities and the Environment, 35*, 163–164.
Wilson-Doenges, G. (2000). An exploration of sense of community and fear of crime in gated communities. *Environment and Behavior, 32*, 597–611.

Further Reading

Low, S. (2004). *Behind the gates: Life, security and the pursuit of happiness in fortress America*. New York: Routledge.
Stephen, M., & Anotti, L. (Eds.). (2013). *Building walls and dissolving borders: The challenges of alterity, community and securitizing space*. New York: Routledge.

Residential Security: Houses and Apartments, Public and Private

Tim Prenzler
School of Law, University of the Sunshine Coast, Sunshine Coast, QLD, Australia

Keywords
Residential security · Home security · Apartment security · Domestic burglary prevention · Securitization · Place management

Definition

Residential security relates primarily to physical protection from external sources of crime-related harms potentially experienced by people in their abode and secondarily includes neighborhood safety as a partial prerequisite for being and feeling safe at home.

Introduction

Various forms of burglary constitute the most common threat to residential security (Weisel 2004). Burglary entails unauthorized access and removal of goods, sometimes simply by trespassing. In other cases, entry is forced – often referred to as "breaking and entering" – and damage to property can ensue even when offenders are unsuccessful in obtaining valuables. Burglars are generally motivated by material gain and focus on targets that are of immediate benefit to them, such as cash or goods that can be easily exchanged for cash (Bennett and Wright 1984; Weisel 2004). Unemployment and social marginalization are common, but not exclusive, factors in offender dispositions (Fallesen et al. 2018). Burglary rates are highly variable although burglary is widely viewed as a "volume crime," and surveys have shown victimization rates as high as 3% and 4% of households per annum in many developed countries (van Dijk et al. 2007, p. 66).

Dwelling places face a number of other security threats apart from burglary. "Home invasions" involve offenders entering a property seeking to obtain cash, drugs, or other goods by threats, sometimes resorting to torture or murder (Heinonen and Eck 2012). Other security breaches extend to graffiti and vandalism, voyeurism, sexual assault, kidnapping, assault, and murder. Multiple dwellings and high-density dwellings can be particularly prone to problems of disorder, excessive noise, drug dealing and consumption, and crime gangs. Residential security issues can also spill over into adjoining streets and parks, where crimes can affect the well-being and safety of residents in the wider neighborhood.

Vulnerability and Opportunity Theories

The best explanation for residential crime and specific vulnerabilities of different premises relates to opportunity factors – primarily low rates of guardianship and poor standards of physical security (Felson 1998; Weisburd et al. 2016). In that regard, the 1960s and 1970s saw a major shift in lifestyles that greatly enlarged opportunities for household crime, especially burglary. Traditional households often had 24-h natural guardianship, with several generations residing under the one roof and women at home engaged

in domestic duties and managing children. People generally stayed home at nights and weekends. The postwar economic boom allowed for greater freedom and mobility, with both parents in the workforce, children in day care and grandparents in retirement villages. This meant that residential areas emptied during the day; and enhanced entertainment and holiday options meant that many places were also unguarded at weekends and nights. Increasing prosperity generated an enormous proliferation of attractive targets in homes, including cash, jewelry, and electrical goods. These have been described as goods *craved* by offenders – that is, they are "concealable, removable, available, valuable, enjoyable and disposable" (Clarke 1999, p. vi).

Research has also shown that perceptions regarding access and egress affect burglars' selection of targets (Weisel 2004). For example, homes on grid pattern streets with multiple access and escape points often have higher rates of burglary compared to those on limited access roads. Cul-de-sacs are particularly well-suited to surveillance of potential offenders. The proliferation of motor vehicles in the postwar boom made a further contribution to ease of access to homes and escape with stolen goods. Motor vehicles on private premises were also an attractive target for thieves. Detached houses in sprawling suburbs provided multiple entry points and access through gardens and yards. However, larger housing complexes, whether private or public, can also be attractive because of limited surveillability and the anonymity provided by multiple occupancy (Armitage 2013). In addition, renting a home, or moving frequently, increases crime risks, with less in the way of personal and financial investments in security (Townsley et al. 2013). Residential burglary is also characterized by high rates of repeat victimization, with offenders gambling on further success against a known target within a few months of an initial burglary (Weisel 2004).

A number of other variables have been identified in residential crime vulnerabilities. In a groundbreaking study illustrating the principles of "Crime Prevention Through Environmental Design" (CPTED), Oscar Newman (1973) identified building design features affecting crime rates in two low-income high-rise "projects" in New York City. Both projects were "almost identical in overall size, density and population characteristics" (p. 38). However, in 1969 the Van Dyke project experienced 1189 crimes, including 52 cases of "malicious mischief" and 92 robberies, while Brownsville had a total of 790 crime incidents (34% less), 28 incidents of malicious mischief (46% less) and 24 robberies (74% less) (Newman 1973, p. 47). Further analysis indicated that the layout of the Van Dyke buildings facilitated crime, largely through offender anonymity, with concealed pathways, entries lacking visibility from the street, and with large load elevators and long corridors in the high towers. Brownsville buildings were lower rise (three to six stories), with observable "zones" and entryways visible from the street and smaller vestibules and elevators that helped residents get to know each other and made strangers or resident offenders stand out. Apart from a crime problem, Van Dyke also had more maintenance problems and a higher rate of tenant turnover.

CPTED principles overlap with the idea of "risky facilities" (Eck et al. 2007). Research in this area has highlighted enormous variation in crime rates between locations with similar functions. Within this concept, poor building design interacts with poor management strategies – such as tolerance of disorderly tenants or failure to provide adequate safety mechanisms. Negligent management practices can function as "crime enablers": high crime locations often have "fewer rules, lax enforcement, easy access, poor security, and other features that help offenders detect targets, commit crimes, and get away" (Eck et al. 2007, p. 240).

The post-1960s crime boom also highlighted the inadequacy of prevention through deterrence and incapacitation by the criminal justice system. In many locations, rates of arrest and conviction for volume crimes such as domestic burglary were as low as 5% (Weisel 2004). The inability of police to provide protection was highlighted in an innovative study by Felson (1998). The study estimated the amount of police on-site protection of premises in Los Angeles County were patrol officers are to be fully deployed. The data showed

that each location would receive 15 seconds of a police presence in 24 h. Doubling police numbers would provide 30 seconds of protection. "like putting two drops in a bucket instead of one" (1998, p. 9).

Home Security and the Crime Drop

A growing realization of the need to prevent crime by alternative or supplementary measures to the arrest and sanctioning strategies of the criminal justice system prompted rapid growth in the security industry internationally from the 1970s (van Dijk 2008). In-house and contract security services provided site-specific tailor-made interventions to close off opportunities for crime. The industry played "catch up" with rising crime rates until the 1990s when its impact became evident in the "international crime drop" (van Dijk et al. 2012). The decline in crime has been associated with diverse factors, including economic cycles, smarter policing, and increased imprisonment. However, analyses by van Dijk (2012) and Farrell (2013) indicated that enlarged "self-protection" strategies and "responsive securitization" provided the best explanation at the global level (van Dijk 2012, pp. 11 and 10).

Residential security provides one of the best examples of "securitization," where the installation of security devices, such as intruder alarms, has coincided with large reductions in burglary rates (van Dijk 2012). A good illustration of this association can be found in a study included in the 2009/10 British Crime Survey report, which found that "Households with 'less than basic' home security measures were six times more likely to have been victims of burglary (5.8%) than households with 'basic' security (0.9%) and ten times more likely than households with 'enhanced' home security measures (0.6%)" (Flatley et al. 2010, pp. 2–3). "Basic security" consisted of "window locks and double locks or deadlocks to outside doors." "Enhanced security" included these and one additional device, such as a security grill, sensor light, or alarm. Longer range analyses of the British survey have shown how the effects of improved security have been concentrated in reduced rates of forced entry and entry into unoccupied dwellings (Tseloni et al. 2017a, b). Offender surveys also support the view that security devices deter and frustrate burglars (e.g., Brown 2015).

Case Studies

The residential security literature includes a variety of case studies of successful security-based interventions. The following summaries provide a sampler of some of the more prominent ones across a diverse range of initiatives. In addition to the correlation studies outlined above, they show significant promise for large-scale benefits from improved target hardening and associated forms of enhanced guardianship.

"The Kirkholt Project," conducted in the late 1980s in the town of Rochdale in England, was focused on addressing high rates of burglary on a housing estate through the multiple situationally-based strategies of "target hardening," "target removal," and increased surveillance (Forrester et al. 1990). The interventions were developed following a diagnostic exercise which highlighted the phenomenon of repeat victimization, often within 6 weeks of the initial offense. Firstly, when a burglary was reported, a crime prevention officer visited the premises within a few days and carried out a security risk assessment. Recommended security upgrades – mainly, it appears, in the form of strengthened doors and locks – were paid for by the housing department of the local council. Secondly, coin-operated fuel meters were removed, and an alternative payment system was adopted. The meters had been attractive targets for thieves. Thirdly, an upgraded form of neighborhood watch was introduced, called "Cocoon Watch." The immediate neighbors of burglary victims were asked to keep a close eye on the burgled property and report questionable activities. Participants were provided with free security upgrades as an incentive and to expand the range of protection. The idea for Cocoon Watch derived from a finding that 70% of entry points used by burglars were visible to neighbors.

It was not possible to separate out the effects of the different strategies in the Kirkholt Project. Nonetheless, the evaluation showed that rates of burglary fell by 75%, from 44 per month in 1986–1987, the year before the project began, to 11 per month in the third year after implementation in 1989–1990 (Forrester et al. 1990, p. 27). This represented "a fall from approximately 25% to 6% per annum of the 2,280 households on the estate" (Tilley 1993, p. 2). In terms of the focus on repeat victimization, a major finding was that multiple victimizations reduced to zero. There was also no evidence of spatial displacement to neighboring locations. A financial cost-benefit assessment found that the interventions generated a total saving of £1.2 million (Forrester et al. 1990, p. 44). (See Cirel et al. 1977 for a similar project in Seattle.)

Another famous anti-burglary project – "Operation Identification" – was carried out in the late 1980s in a small community in Wales (Laycock 1997). The project sought to reduce the potential rewards from theft by creating a link between offenders and stolen property. Residents were visited by police and special constables who offered the free use of property marking equipment. On a return visit, officers inventoried the marked property. Deterrence was enhanced through extensive publicity and decals on doors and windows, and household participation rates reached 72%. The evaluation showed that there had been 91 burglaries among participating households in the year before the intervention. This reduced by 61% to 35 burglaries in the following year, with no evidence of displacement. In nonparticipating households, the victimization rate remained stable at 37 incidents before and 39 after the intervention.

A famous study of the effects of lighting is particularly interesting because its scope extended beyond individual homes to diverse crime types in a neighborhood area where up to 70% of crime occurred at night. Painter and Farrington (1997) reported on the introduction by the local authority of improved street lighting in the public housing estate of Dudley in England in the early 1990s. Natural surveillance was enhanced through upgraded lighting that greatly improved visibility. Surveys of residents were conducted in the experimental site and a control site in the year before and the year after installation. In the experimental site, victimization was reduced by 23% from 42% of survey respondents to 32%, whereas victimization in the control site dropped by 3% from 39% to 38%. (See also Painter and Farrington 2001 on positive results from a similar project in Stoke-on-Trent.)

A number of successes have also been attributed to the application of "Secured by Design" standards. This involves government certification of buildings that comply with a variety of CPTED and security hardware standards, often introduced as a police-led initiative (Hicks and Sansfaçon 2002). Certification normally attracts lower home insurance premiums. The Dutch Secured Housing label was introduced in 1989 and applied to new housing estates. It has been claimed that "the risk of dwellings being burgled . . . dropped significantly by 95% in new estates and 80% in existing environments" (Jongejan and Woldendorp 2013 p. 31). A case study evaluation of a program introduced in Rotterdam area in 1991 reportedly found that "Compared to households that did not participate in the program . . . households in the Secured Label program had a 70% reduction in burglaries . . . while rates of burglary were increasing countrywide" (Hicks and Sansfaçon 2002, p. 15). More broadly, a 2010 study found that, since a 1999 regulation extended required door and window security standards to all newly built homes, the burglary rate in this category fell "from 1.1 to 0.8 annually, reduction of 26%," without evidence of displacement (Vollaard and van Ours 2011, p. 1). Positive results have also been observed with the Secured by Design (SBD) scheme in the United Kingdom. For example, a study in West Yorkshire found that non-SBD properties experienced 22.7 burglaries per 1000 properties in 1 year compared to a rate of 5.8 for SBD compliant locations (Armitage and Monchuk 2011, p. 332; see also Armitage 2013).

Recognition of the problem of "risky facilities" (above) and management neglect stimulated innovations in holistic "place management" for improved amenity and security (Eck et al. 2007). In some cases, in a strategy referred to as "Third Party Policing," more responsible security-

focused management has been generated by police and local government pressure on landlords (Mazerolle and Ransley 2006). In other cases, landlords have initiated reforms in response to recurring problems. A good example is a management-focused program to address high crime rates and resident alienation in the large Mitchellhill public housing estate – consisting of five 19-story tower blocks – in Glasgow in 1989. The program involved the introduction of an on-site manager and assistant, together with 12 concierges who provided 24-h security-oriented services to residents (Davidson and Farr 1994). Other innovations included security hardware such as solid doors with barrel locks (which could be rekeyed for new tenants), better lighting, CCTV, controlled entry to foyers, and removal of internal landing doors that provided hiding places, along with increased police patrols and a "multi-watch" system for residents to report issues to police. Efforts were also made to improve the attractiveness of the estate with renovations and provision of furnished flats and tenant representation on the tenant selection committee.

An initial evaluation of the Mitchellhill program found that the total number of police-recorded crimes fell by 62% from 141 over 15 months to 53 in an equivalent period following the introduction of the concierge scheme (Davidson and Farr 1994, p. 26). In the same time periods, burglaries reduced by 71%, and theft of vehicles and theft from vehicles reduced by 72%. Large reductions in maintenance costs, mainly associated with vandalism, were also recorded, along with increased demand for flats, increased occupancy, and increased rental income. Program costs after savings were put at approximately £2 per flat per week (p. 33). Crime rates remained stable over the same period in a nearby comparable area. A brief follow-up evaluation, using 1991 and 1992 data, showed a partial regression, with the overall crime rate back up to approximately 50% of the pre-intervention rate. However, the large reductions for burglary and vehicle-related crime held firm (p. 33).

In an important sub-category of residential security applications, case studies have emerged in recent years of interventions to reduce repeat domestic violence and provide a safe setting for victims of family violence to rebuild their lives (Prenzler and Fardell 2017). Programs usually work through free security hardware upgrades on victims' homes, including rental accommodation, to protect against a range of threats and intrusions that can follow from separation and adoption of a protection order – including harassment, abduction, assault, and murder. Although available studies have not included control groups, a review of six within-group evaluations showed consistent extremely positive outcomes for participants in terms of reduced offenses and improved feelings of safety, including for children (Prenzler and Fardell 2017). Monitored duress alarms, with a police priority protocol, appeared particularly valuable in supplementing target hardening. Safety in domestic violence shelters also represents an important sub-category of residential security, entailing the need to integrate high security standards with the needs of clients – often including children – for privacy, amenity, and easy access (Gierman and Liska 2013).

Conclusion: Best Practice Principles

The research on residential security has generated a number of valuable guides for optimizing prevention (e.g., Draper et al. 2017; Heinonen and Eck 2012; Sampson 2001; Weisel 2004; see also Security Management, Physical Security: Best practices, Physical Security: Audits). An important principle involves making the best use of available target hardening devices to optimize deterrence and denial of offenders – ensuring equipment is of quality design and materials with no gaps allowing easy access. More generally, design principles emphasize the value of "defence in depth," beginning with appropriate access control measures at the perimeter of a residential setting. Concentric rings of protection allow for the operation of the "5 Ds" of physical security: "deter, detect, deny, delay and defend" (Marier 2012, pp. 1–2). Each layer of protection should operate to impede or block an intruder's progress toward targets, as well as impeding their escape. High-grade detection systems and target

hardening are particularly important in the defense of high-value assets.

Most importantly, however, guides generally emphasize the necessity of a problem-solving process in diagnosing residential crime problems and risk factors, including resident input, matching interventions to risk, engaging in regular system tests to ensure currency, and balancing security with amenity and fire safety criteria. Making the most of security technology as it improves in quality and becomes more affordable and convenient is also fundamental to a "continuous improvement" process. For example, innovations in CCTV functionality now allow for internet-based remote verification of alarm activations on computers and mobile phones, substantially mitigating the long-term problem of false intruder alarm activations and ensuring a valid rapid response from police or security firms (Sampson 2011).

Residential security can also be enhanced through collective efforts. Small regular financial contributions by residents of apartment buildings allow for the engagement of security firms and/or the employment of a facilities manager or concierge with security duties (Townsley et al. 2013). This can also work in "gated communities" of detached or semidetached houses. In these contexts, the concept of crime prevention through effective "place management" has enormous potential (Eck et al. 2007).

Finally, it should be noted that many advocates of securitization for residential crime prevention also adopt both pragmatic and social justice imperatives in support of welfare programs to address poverty and neglect as causes of both victimization and offending (e.g., Forrester et al. 1990). Offender motives can be addressed through a variety of social support measures, including employment programs (Fallesen et al. 2018). Victim vulnerability can also be addressed through enhanced employment, as well as subsidized security and mandated security standards in public housing – possibly obviating the need for alienating crime prevention measures such as segregated high security communities. The case studies described above also demonstrated the value of crime prevention partnerships in bringing together groups such as police, local government, tenants, security companies, and charities (such as domestic violence support services) in addressing residential security challenges.

Cross-References

- ▶ Criminals: Blue-Collar Crimes
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Methods and Practices
- ▶ Security Management

References

Armitage, R. (2013). *Crime prevention through housing design: Policy and practice*. Houndmills: Palgrave Macmillan.

Armitage, R., & Monchuk, L. (2011). Sustaining the crime reduction impact of designing out crime: Re-evaluating the secured by design scheme 10 years on. *Security Journal, 24*(4), 320–343.

Bennett, T., & Wright, R. (1984). *Burglars on burglary: Prevention and the offender*. Brookfield: Avebury Publishing.

Brown, R. (2015). Explaining the property crime drop: The offender perspective. *Trends and Issues in Crime and Criminal Justice, 495*, 1–7.

Cirel, P., Evans, P., McGillis, D., & Whitcomb, D. (1977). *Community crime prevention program – Seattle, Washington – Exemplary project*. Washington, DC: National Institute of Law Enforcement and Criminal Justice.

Clarke, R. (1999). *Hot products*. London: Home Office.

Davidson, J., & Farr, J. (1994). Mitchellhill estate: Estate-based management (concierge) initiative. In S. Osborn (Ed.), *Housing safe communities: An evaluation of recent initiatives* (pp. 22–33). London: Safe Neighbourhoods Unit.

Draper, R., Ritchie, J., Wilson, E., & Prenzler, T. (2017). Best practice in physical security and people management. In T. Prenzler (Ed.), *Understanding crime prevention* (pp. 151–166). Brisbane: Australian Academic Press.

Eck, J., Clarke, R., & Guerette, R. (2007). Risky facilities. *Crime Prevention Studies, 21*, 225–264.

Fallesen, P., Geerdsen, L., Imai, S., & Tranæs, T. (2018). The effect of active labor market policies on crime: Incapacitation and program effects. *Labour Economics, 52*, 263–286.

Farrell, G. (2013). Five tests for a theory of the crime drop. *Crime Science, 2*(5), 1–8.

Felson, M. (1998). *Crime and everyday life*. Thousand Oaks: Pine Forge Press.

Flatley, J., Kershaw, C., Smith, K., Chaplin, R., & Moon, D. (2010). *Crime in England and Wales 2009/10*. London: Home Office.

Forrester, D., Frenz, S., O'Connell, M., & Pease, K. (1990). *The Kirkholt burglary prevention project: Phase II*. London: Home Office.

Gierman, T., & Liska, A. (2013). *Shelter for women and girls at risk of or survivors of violence*. Ottawa: Canadian Network of Women's Shelters & Transition Houses.

Heinonen, J., & Eck, J. E. (2012). *Home invasion robbery*. Washington, DC: US Department of Justice.

Hicks, D., & Sansfaçon, D. (2002). *Preventing residential burglary and home invasions*. Montreal: International Centre for the Prevention of Crime.

Jongejan, A., & Woldendorp, T. (2013). A successful CPTED approach: The Dutch 'police label secure housing'. *Built Environment, 39*(1), 31–48.

Laycock, G. (1997). Operation identification, or the power of publicity? In R. Clarke (Ed.), *Situational crime prevention: Successful case studies* (pp. 227–234). Albany: Harrow and Heston.

Marier, K. (2012). *The 5 Ds of outdoor perimeter security*. Retrieved from http://www.securitymagazine.com/articles/82833-the-5-d-s-of-outdoor-perimeter-security

Mazerolle, L., & Ransley, J. (2006). *Third party policing*. Cambridge: Cambridge University Press.

Newman, O. (1973). *Defensible space: Crime prevention through environmental design*. New York: Collier Books.

Painter, K., & Farrington, D. (1997). The crime reducing effect of improved street lighting: The Dudley project. In R. Clarke (Ed.), *Situational crime prevention: Successful case studies* (pp. 209–226). Albany: Harrow and Heston.

Painter, K., & Farrington, D. (2001). The Financial benefits of improved street lighting, based on crime reduction. *Lighting Research Technology, 33*(1), 3–12.

Prenzler, T., & Fardell, L. (2017). Situational prevention of domestic violence: A review of security-based programs. *Aggression and Violent Behavior, 34*(1), 51–58.

Sampson, R. (2001). *Drug dealing in privately owned apartment complexes*. Washington, DC: US Department of Justice.

Sampson, R. (2011). *False Burglar alarms* (2nd ed.). Washington, DC: US Department of Justice.

Tilley, N. (1993). *After Kirkholt – theory, method and results of replication evaluations*. London: Police Research Group, Home Office.

Townsley, M., Reid, S., Reynald, D., Rynne, J., & Hutchins, B. (2013). *Crime in high rise buildings: Planning for vertical safety*. Canberra: Australian Institute of Criminology.

Tseloni, A., Farrell, G., Thompson, R., Evans, E., & Tilley, N. (2017a). Domestic burglary drop and the security hypothesis. *Crime Science, 6*(3), 2–17.

Tseloni, A., Thompson, R., Grove, L., Tilley, N., & Farrell, G. (2017b). The effectiveness of burglary security devices. *Security Journal, 30*(2), 646–664.

van Dijk, J. (2008). *The world of crime*. Thousand Oaks: SAGE.

van Dijk, J. (2012). *Closing the doors: Stockholm Prize-winners lecture 2012*. Paper presented at the Stockholm Criminology Symposium, Stockholm.

van Dijk, J., van Kesteren, J., & Smit, P. (2007). *Criminal victimisation in international perspective: Key findings from the 2004–2005 ICVS and EU ICS*. Tilburg: Tilburg University & United Nations Office on Drugs and Crime.

van Dijk, J., Tseloni, A., & Farrell, G. (2012). *The international crime drop: New directions in research*. London: Palgrave Macmillan.

Vollaard, B., & van Ours, J. C. (2011). Does regulation of built-in security reduce crime? Evidence from a natural experiment. *The Economic Journal, 121*(552), 485–504.

Weisburd, D., Eck, J., Braga, A., Telep, C., Cave, B., et al. (2016). *Place matters*. New York: Cambridge University Press.

Weisel, D. L. (2004). *Burglary of single-family houses*. Washington, DC: US Department of Justice.

Further Reading

Bottom, N. (2012). Multi-residential security. In L. Fennelly (Ed.), *Handbook of crime prevention and loss prevention* (pp. 457–465). Burlington: Elsevier.

Zahm, D. (2007). *Using crime prevention through environmental design in problem-solving*. Washington, DC: US Department of Justice.

Retail Security: Employee Theft

Lauren R. Shapiro
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Internal retail crime · Fraudulent disbursements · Intellectual theft · Embezzlement · Larceny · Skimming

Definition

Retail employee theft involves "the theft of anything of value from the retailer by an employee or accomplice" (Mishra and Prasad 2006, p. 817). Five specific crimes are categorized under employee theft or asset misappropriation – fraudulent disbursements, intellectual theft, embezzlement, larceny, and skimming (Bailey 2006).

Introduction

Employee theft includes misappropriation of tangible and nontangible assets through fraudulent disbursements (e.g., paid for time not worked), intellectual theft (e.g., selling information to competitor), embezzlement (e.g., stealing cash), larceny (e.g., stealing merchandise), and skimming cash from the register (Bailey 2006). Retail stores sell a variety of goods (e.g., clothes, food, drugs, music, candy) for public consumption and use but lose a significant portion of their profits due to employee theft (Martin et al. 2014). Retailers purport that embezzlement, larceny, and skimming by employees, either alone or in collusion with accomplices, likely accounted for one-third to two-fifths of their cash and merchandise losses (see Hayes, Weitz, & Hollinger's National Retail Security Survey, reported in Martin et al. 2014). This belief is consistent with research findings that internal theft was the second leading source of merchandise shrinkage. According to the 2018 National Retail Security Survey of 63 retailers (Moraca and Hollinger 2018), employee theft comprised 33.2% of the $46.8 billion in economic loss for the retail industry in the USA alone. This estimate of loss from employee theft reflected a slight increase from the year before but represented a decline from the rates of 35.8% in 2016 and 34.5% in 2015 (Moraca and Hollinger 2018).

Retailers are concerned about the number of employees involved, how often they steal, and the length of time they offend prior to being apprehended. A recent examination of federally processed cases revealed that one-third to three-fourths of employees commit employee theft at least once, and for 28.7% of the retail cases, theft occurred repeatedly over months or even years (Karpp 2017). The length of time employee theft continues may depend on whether other employees witness it and are willing to report it. According to Kessler International (2013, as cited in Martin et al. 2014), 45% (225 out of 500) of employees in retail and service companies were aware of or witnessed employee theft. Employees are in a good position to report crimes to their employers and will do so when the organizational climate is conducive with this behavior (Avery et al. 2012). For example, 53% of the tips that led to the initial detection of occupational fraud came from employees reporting other employees (The Association of Certified Fraud Examiners/ACFE 2018), whereas 54% of retail employee theft had been detected by the management (Fikes 2009).

To combat employee theft, the majority of retailers rely on the services and investigations of loss prevention personnel (see ▶ "Retail Security: Use of Security Guards" and ▶ "Security Guards: Authority and Power" chapters in this volume). According to a study by Moraca and Hollinger (2018), 63 retailers indicated that their 2018 loss prevention staffing and budgets, which averaged 0.74% of their sales, either remained constant (44.4% and 42.9%, respectively) or showed growth of 35.5% (for both). Retailers also increased their use of loss prevention systems, such as closed-circuit television/CCTV (27%), training announcements (15.9%) and videos (9.5%), and theft deterrent devices (7.9%), which also affected both shrinkage and offender apprehensions (Moraca and Hollinger 2018). The combination of LP management strategies, reliable electronic article surveillance (EAS) systems, and CCTV placement and use has been credited with reducing retail shrink from all sources (R. McCrie, January 11, 2019, personal communication).

Despite retailers' efforts in prevention, detection, and investigation of loss, employee theft is still a major concern. Employee theft contributed to a 5% loss of businesses' annual revenues, resulting in a global loss in the trillions and led to bankruptcies in various small businesses that included retail, manufacturing, trade, and service companies (Kennedy 2017). Moraca and Hollinger (2018) reported that the responses against dishonest employees, such as average number of apprehensions (506.1 vs. 834), terminations (397.8 vs. 651.6), prosecutions (104.4 vs. 209.6), and civil demands (125.1 vs. 344.5), declined in 2018 compared to 2015. In contrast, a larger investigation using a base of 1.4 million employees at 21 large retail companies with 16,409 stores (the

30th Annual Retail Theft Survey, Jack L. Hayes International 2018) found that 40,286 of the employees who committed theft were apprehended in 2017, roughly accounting for 1:35 employees and resulting in the recovery of nearly $38 million dollars. The conundrum for retailers, whose goal is to reduce loss, is determining whether they should focus more on internal rather than external theft or simultaneously attend to both. Based on the 2017 survey results, retailers were able to increase apprehensions and recover losses by eliminating dishonest employees quickly, launching investigations by specialized loss prevention personnel, and installing software geared to identify dishonest employees (Jack L. Hayes International 2018). This entry focuses on describing employee demographics, motives, and crime methods. It also provides legal responses for retail employee theft and suggestions to improve effectiveness in reducing employee theft.

Descriptive Characteristics of Employee Thieves

Researchers have linked specific characteristics – age, sex, ethnicity, tenure or seniority, and position – to employee theft, but keep in mind the relationship of these variables represents correlations rather than causal factors. It is also important to note that demographic features of employee age, sex, and ethnicity of retail employee thieves are contingent upon the distribution of those features in (a) the area residents who comprise the applicant pool for employment and (b) those apprehended employees (i.e., not all of them will be caught; thus, their characteristics will be missing or misrepresented). For example, ACFE (2018) reported that men comprised the highest proportion of occupational fraudsters in every country from 2008 to 2018, but the proportion varied by region (e.g., 58% in the USA, 69% in Canada, 77% in Western Europe, 92% in Middle East and North Africa).

With those caveats in mind, an overall description of employee thieves as young men, ages 18–22 years, with low-level employment positions held for a short term is based on data from two studies. Fikes (2009, p. 32) examined 502 dishonest retail employees (ages 16–55 years) who were apprehended, investigated, and terminated for theft (i.e., cash, merchandise, rewards abuse, services, point-of-sale abuse) from July 2007 to June 2008. She reported that the offenders in her sample were *white* (55%), *men* (59%), and *young* (48% were between ages 18 and 22 years old). In terms of their employment, they were mainly *low-level positions* (88% hourly employment hourly) with *short-term tenure* (36% up to 6 months).

Baxter (2014) used 678 case reports of dishonest employees (ages 18–47 years) apprehended from 2005 to 2012 from a retail chain with 1089 stores operating in the USA, Puerto Rico, and Canada, specializing in young adult apparel. The typical employee thief was *male* (53%) and *young* (M age = 23 years, $S.D.$ = 4.77, most often ranging from 19 to 22 years based on 678 cases). They commonly held low-to-middle-level positions as marginal/sales associates (61.5%) or as assistant managers (25.9%) but were most likely to have short-term employment tenure (ranging from 2 to 9 months for 156 cases).

In comparison to older employees who have been with their company for a long time, younger employees who have worked a short time period are more likely to commit employee theft (Kennedy 2017). There is some evidence to show that older employees exert positive, moral influence over their younger colleagues by discouraging theft, perhaps resulting from the development with age of crystalized intelligence that fosters their ethical and responsible beliefs and behavior (Avery et al. 2012).

These characteristics may impact employee theft differently when considered in light of other aspects, such as company size. Karpp's (2017) analysis of 104 federal court cases of retail employee theft revealed that most embezzlements were committed by low-level employees (65%), especially those in companies with less than 100 employees (76%). Employee sex also covaries with the size of the company. Karpp (2017) reported that 50.2% of small business thieves were women, but 54.7% of large business thieves were men. Company size also interacted with age and sex. The median age of

female employee thieves was 48 for small businesses, but 43 for large businesses, whereas the median age for male employee thieves was 49 regardless of business size.

Employee theft was affected by the number of employees involved (e.g., collusion) and one's employment position. An examination of 90 Canadian cases of occupation fraud (post 2004) by Peltier-Rivest and Lanoue (2011) revealed that employees were more likely to steal alone than with accomplices, but the average and median loss was higher for the latter than for the former. They also reported that the median loss was usually higher for men than for women, which they attributed to limited employment position within the organization resulting in fewer opportunities for women than for men to have access to and control over large cash amounts. Large economic losses through fraud and embezzlement were often associated with those in a position of authority and financial control (e.g., owners, managers, executives), who were successful at stealing without detection because they knew the loss prevention system so well (Kennedy 2017) and had greater access to company assets than lower level employees (Peltier-Rivest and Lanoue 2011). Education level has also been positively related to employee theft, but this is likely due to the relationship between academic requirements for higher level employment opportunities.

Typical Motives for Employee Theft

Employees have a variety of motives for behaving dishonestly, such as engaging in stealing (i.e.,property deviance) and/or being counterproductive (i.e., production deviance) at work that stem from both individual and organizational factors (Martin et al. 2014; Moorthy et al. 2015). The relationship between property and production deviance is 0.48, and employee dissatisfaction at work may prompt motivation for employee theft (Hollinger and Clark 1983, as cited in Baxter 2014). Retail employees engage in theft based on three individual components – *financial need*, *opportunity*, and *personal characteristics* (Baxter 2014; Martin et al. 2014; Moorthy et al. 2015). Employees' debts and expenses, particularly when they are financially desperate (e.g., due to gambling and/or substance addictions), play a major role in fraud (Baxter 2014; Moorthy et al. 2015). However, most employees will not resort to theft unless presented with opportunity, such as failure to supervise, check, audit, or inventory (Baxter 2014; Martin et al. 2014; Moorthy et al. 2015). Employees who exhibit negative personal characteristics, such as greed, entitlement, lying, deceitfulness, and impulsivity, may commit theft and fraud, especially when surrounded by other employees engaged in similarly deviant behaviors (Martin et al. 2014; Moorthy et al. 2015).

Employee theft is also effected by organizational factors of *compensation*, *justice*, and *ethical work climate* (Baxter 2014; Moorthy et al. 2015). The perception that the employee is not compensated fairly for the work he/she produced may motivate theft as a means of restoring equity (Chen and Sandino 2012). As employee wages were negatively correlated with employee theft, high pay and quality of employees (relative to their peers) were associated with low occurrence of employee theft (Chen and Sandino 2012). Employee theft may also be motivated by the perception that the organization does not treat staff fairly and justly (Moorthy et al. 2015). Employees will work hard, be productive, and be absent less when compensated fairly and treated justly but may seek revenge when they are not (Martin et al. 2014; Nemeth 2019). Another motive for employee theft stems from the organization's ethical work climate as honest or dishonest (Moorthy et al. 2015). Employee theft is likely to be facilitated and maintained when the perception is that the actions themselves are low risk. Moorthy et al. (2015) explain that employees determine whether to engage in theft based on whether coworker theft occurs and is punished; stealing is easy to do because of lack of internal controls (e.g., policies, practices, and procedures), such as formal monitoring (e.g., hidden surveillance); and intention to steal is present.

Methods for Employee Theft

Kessler International (2013 as reported in Martin et al. 2014) indicated that nearly 475 out of 500 respondents from retail and service companies admitted to *production deviance*, specifically stealing time (e.g., 30% falsified time worked, including taking unauthorized breaks, 63% checked social media sites during work day) and *property deviance*, including taking office supplies and services (e.g., pens, paper, notepads). To understand employee theft, loss prevention personnel should acquaint themselves with the five typical methods, which can be categorized as "intangibles," such as fraudulent disbursements and intellectual theft, and "tangibles," such as skimming, embezzlement, and larceny/theft (Bailey 2006).

According to Mishra and Prasad (2006), *fraudulent disbursements* refer to misappropriation of assets by employees and involve multiple on-book fraud schemes (see Table 1 for a description of these methods). Employee thieves falsify store records to conceal the loss of merchandise or cash. Although it is impossible to determine how much loss is due to fraudulent disbursements from the various schemes, it is likely that some if not all of it is encompassed in the combined administrative/paperwork error (18.8%), vendor fraud/error (5.8%), and unknown error (6.6%) as indicated by retailers in 2018 (Moraca and Hollinger 2018). *Intellectual property theft* refers to stealing a company's trade secrets, including ideas, products, and strategies for the sale of these products (see Table 1). Kennedy (2017) reported that 4.5% of the employee thefts in his study of small retail and nonretail businesses involved intellectual property.

Within retail stores, employee theft of tangibles from highest to lowest degree is checkout, sales floor, and customer service (Mishra and Prasad 2006). For example, Fikes (2009) indicated that 38% of employee theft was point of sale, 26% was merchandise theft, and 24% was rewards abuse. Performing refund fraud was the second most common method of employee fraud in retail stores found in Baxter's (Baxter 2014) study, accounting for 34.8% of the cases (pp. 164–167). Baxter also reported that the highest incident rates for retail employee theft were stores in suburban (55%) and mall locations (78.7%).

Kennedy (2017) specified that cash, ranging from $5 to $2 million, was the most stolen object by employees in small retail and nonretail businesses (43.2%). As indicated on Table 1, cash theft is predominantly obtained through two methods – skimming and embezzlement. *Skimming* occurs when cash is taken by the employee at the point of sale but before it is recorded. *Embezzlement* refers to theft by a retail employee who has legal access to the property, such as a cashier who takes cash from the register, whereas a store clerk who takes money from the register is committing property theft or larceny.

Retail employees also commit *larceny* when they steal or fail to pay for merchandise or discount merchandise for themselves or others without authorization (Mishra and Prasad 2006). Larceny is categorized under property crime offenses and is defined as the "unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another" (Federal Bureau of Investigation 2016) with felonious intention (Nemeth 2018). The level of severity for larceny –misdemeanor or felony – depends on the dollar value of the items, but the criteria are determined by jurisdiction. Baxter (2014) found that employee theft was committed primarily by passing or removing merchandise from the store in 52.5% of the cases (pp. 164–167). Employee theft of merchandise through sweethearting contributes significantly to retail shrink. "Sweethearting," the practice of giving customers unauthorized free (e.g., samples) or discounted merchandise, contributes up to 35% of profit losses that totals billions, mainly because it is seen by employees as promoting customer satisfaction (Martin et al. 2014).

Many employee theft incidents are not one-time incidents (Karpp 2017). For example, Kennedy (2017) found that most of the 44 retail and nonretail employee thefts reported were ongoing schemes (59.1%) lasting on average 16 months (range of 2 weeks to 20 years). Similarly, a recent report by the ACFE (2018) showed

Retail Security: Employee Theft, Table 1 Criminal Offenses and Methods

Criminal offense	Methods
Fraudulent disbursements	Payments to the employee using his/her employment position to obtain payment for inappropriate purposes, including: (a) Check tampering schemes (e.g., forging signature of payee or endorser for oneself or accomplices; cashing fraudulent checks; reissuing outstanding checks; account and wire transfers paid to themselves) (b) Billing schemes (e.g., false vendor payments to themselves or accomplices, petty cash disbursements) (c) Payroll schemes (e.g., forged payroll checks, commission payments not earned, checks to terminated employees, overtime for time not worked, worker's compensation) (d) Expense reimbursement schemes (e.g., payment for expenses never incurred; duplicate payment) (e) Register reimbursement schemes (e.g., coupon stuffing, credit card reimbursement to self or accomplices, stealing customer credit card information) (f) Misusing benefits and policies (e.g., medical and healthcare frauds including undeserved sick leave or vacation days) (g) Tax-related frauds (e.g., charitable and religious contribution frauds) (h) Insurance fraud (e.g., false claims of amount and/or cost of merchandise and cash loss) (i) Forgery and document tampering (Mishra and Prasad 2006; Nemeth 2019)
Intellectual property theft	Taking intangible assets, such as corporate information, that give a competitor an advantage over the retailer, including: (a) Proprietary information/products (b) Client lists (c) Marketing plans (Martin et al. 2014)
Skimming	Cash is pocketed by cashier or manager prior to it entering the register (without record) to deprive the merchant from full retail price by personally or in consort with another: (a) Voiding sale (b) Hitting "no sale" (c) Overcharging (d) Shortchanging (e) Under ringing (f) Crediting for nonexistent returns (g) Getting refunds using discarded customer receipts (ACFE 2018; Mishra and Prasad 2006; Nemeth 2018, 2019)
Embezzlement	Cashiers and/or managers (who have authority to handle money) take cash from the register, safe, or bank deposit bag (Mishra and Prasad 2006)
Property crime: larceny retail theft offense [specialized statute]	Thief takes possession of, carries away, or transfers merchandise without paying full retail price by personally or in consort with another: (a) Altering, transferring, or removing price tag (b) Transferring merchandise from original container to another container or a concealed location (including bag, box, or garbage for later retrieval) (c) Making inoperable inventory control tag or security strip (d) Taking merchandise through unsupervised exits (e) Stealing from returned goods and layaway (f) Shipping stolen merchandise to their own address (g) Damaging merchandise purposefully to purchase at discount and/or substituting damaged merchandise for undamaged goods (Nemeth 2018, 2019)

that employees were able to avoid detection on average for register disbursements and on-hand cash about 12 months, for noncash theft and skimming about 18 months, and for cash larceny about 24 months.

Retailer Responses to Employee Theft Within the Law

A professional investigation is conducted to determine whether employee theft has occurred

(see ►"Investigations: Employee Theft of Employer Property" chapter in this volume). Once confirmed, then retailers may pursue criminal charges through prosecution and/or file for civil recovery to obtain restitution for losses (Fikes 2009) (see ►"Investigations: Criminal", ►"Investigations: Employee Theft of Employer Property", ►"Investigations: Criminal", and ►"Law: Administrative" chapters in this volume). To file criminal charges, two types of evidence are required. First, there must be documents, video, or written admission by the employee that the merchandise offered for sale, stored, or on display was taken (i.e., be in possession of it). Second, it must be shown that the employee intentionally deprived the owner of it by (willfully) carrying it away, concealing it, converting it (i.e., altering the price of the merchandise, removing the inventory control tag, or making the tag inoperable), or failing to pay for it (International Association of Professional Security Consultants/IAPSC 2015, p. 3; Nemeth 2018, p. 171).

Kennedy (2017) reported that only 16% of the 64% of small businesses (retail and nonretail) who experienced employee theft reported it to police. In their examination of occupational fraud, ACFE (2018) reported that the pursuit of criminal charges had declined over the past 10 years (69% in 2008 to 58% in 2018, p. 48). Yet, when criminal cases were presented to the prosecutor, most of them were accepted for trial (82%), mainly resulting in guilty/no contest pleas (53%) and convictions (20%), with only a 1% acquittal (ACFE 2018, p. 49).

Even when investigations yield the requisite evidence for prosecuting the employee, other factors should be considered. Specifically, the amount of time involved of the owner/manager and other employees in the prosecution process, including interviews by the police and court appearances, as well as economical considerations due to the cost of wages and travel payment for the witnesses, help determine this decision. Unfortunately, even when the trial yields a guilty verdict (or the defendant takes a plea), the judge may sentence the defendant to jail, prison, or even probation but may not include restitution. ACFE (2018) indicated that only 15% of companies recovered all of their losses; most companies recovered none (53%) or some (32%) of their losses from occupational fraud (p. 51).

Retailers who wish to consider pursuing criminal charges must also balance the evidence against the cost of the merchandise in determining what benefit legal charges will have. For example, Fikes (2009) reported that the majority of cases involved losses of up to $24 (39%) and between $25 and $199 (20%), which likely discouraged the retailer to prosecute. ACFE (2018) indicated that recovery was negatively related to the amount of the loss, such that 30% of companies recovered all of their losses if it was under $10,000, but only 8% were able to do so if the loss was over a million dollars (p. 51).

Employers decide against filing charges of occupational fraud against employees based on their desire to sever ties quickly through firing the employee, particularly due to the emotional strain of the betrayal, their beliefs that the police are ineffective, or because their attorneys advised against it (Kennedy 2017). ACFE (2018, p. 50) indicated that the top three reasons that companies chose not to involve law enforcement were impact of bad publicity (38%), belief that internal discipline resolved it (33%), and the cost (24%). Instead, companies chose simply to terminate employees for retail theft (87%, Fikes 2009) and fraud (65%, ACFE 2018), without filing charges. Termination as a punishment, however, was mediated by the offender's position in the company (ACFE 2018, p. 48), such that it was more likely at the employee and manager levels (e.g., 72% and 67%, respectively) than at the owner/executive levels (44%).

An alternative to criminal prosecution is civil lawsuit; this remedy will allow the retailer to be reimbursed for the cost of the stolen merchandise and sometimes even the cost of the investigation. The results from the ACFE (2018) survey indicated that about a quarter of the fraud cases against employees were processed through civil suits, with favorable judgments for the retailer (53%) or through settlement (27%). Voluntary restitution involves the employee returning merchandise that is still in saleable condition that they

or others still possess, including in pawnshops. Employees may also make restitution using their final paycheck and unused benefits (e.g., holiday pay). To determine which solution for employee theft is best for the retailer, guidelines should be created in conjunction with representatives from Human Resources, Loss Prevention, and Operations.

Conclusion

Organizations struggle with the issues of trust and balancing relations between supervisors and employees, decisions of punishment and restitution, and how best to implement security prevention and detection tools (Cunningham 2017). Employee theft and the methods employed to counter it contribute to 30% of businesses becoming bankrupt, nearly closing, or failing, as well as employee layoffs and loss in bonuses and raises (Mishra and Prasad 2006). Communities lose important revenue though commercial taxes on the items that were stolen instead of being purchased and on income taxes from stores when retailers move out of the neighborhood due to the high losses suffered from employee theft. Store closings, in turn, increase unemployment for those in the affected areas, as well as impact the economic well-being of the nation.

Applying a routine activities theory approach, employee theft occurs when a suitable target is available, the offender is motivated, and a capable guardian is absent (Martin et al. 2014). Fikes (2009) found that managements' failure to adhere to policy and procedures provided associates with the opportunities to steal for 77% of the cases. Each organization must examine their own cases of employee theft to determine which situational and behavioral factors played a role (Kennedy 2017). Retailers must then implement individual- and organizational-level changes to counter employee theft, such as increasing perception of punishment as certain and swift; prescreening employees; using technology (CCTV), random inventory checks, peer detection, and control; and creating a culture of intolerance for employee fraud and abuse (Avery et al. 2012; Kennedy 2017). By closing the gap (i.e., hardening the target, reducing motivation for the offender, and increasing the guardian's effectiveness), retail shrink through employee theft can be reduced.

Cross-References

- ▶ Investigations: Criminal
- ▶ Investigations: Employee Theft of Employer Property
- ▶ Law: Administrative
- ▶ Retail Security: Use of Security Guards
- ▶ Security Guards: Authority and Power

References

Association of Certified Fraud Examiners/ACFE. (2018). *Report to the nations: 2018 global study on occupational fraud and abuse*. Accessed at: https://www.forensicaccounting.com.au/wp-content/uploads/2018/05/2018-report-to-the-nations.pdf. 26 Nov 2018.

Avery, D. R., McKay, P. F., & Hunter, E. M. (2012). Demography and disappearing merchandise: How older workforces influence retail shrinkage. *Journal of Organizational Behavior, 33*, 105–120.

Bailey, A. A. (2006). Retail employee theft: A theory of planned behavior perspective. *International Journal of Retail & Distribution Management, 34*(11), 802–816.

Baxter, D. N. (2014). Who is taking the shirt off your back? A multi-method analysis of theft at a specialty retailer. Dissertation, Indiana University of Pennsylvania. Accessed at: https://knowledge.library.iup.edu/cgi/viewcontent.cgi?article=1153&context=etd. 26 Nov 2018.

Chen, C. X., & Sandino, T. (2012). Can wages buy honesty? The relationship between relative wages and employee theft. *Journal of Accounting Research, 50*(4), 967–1000. https://doi.org/10.1111/j.1475-679X.2012.00456.x.

Cunningham, K. P. (2017). *Perceptions of the impact of employee theft within small businesses: A multiple case*. A dissertation submitted to Northcentral University, San Diego California. ProQuest No. 10689819.

Federal Bureau of Investigation. (2016). 2016 crime in the United States. U.S. Department of Justice. Available at: https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/larceny-theft. 5 July 2018.

Fikes, E. M. (2009). Dishonest associates in the workplace: The correlations between motivation and opportunity in retail among employee theft. Dissertation, The University of Texas, Arlington.

Accessed at: https://rc.library.uta.edu/uta-ir/bitstream/handle/10106/1650/Fikes_uta_2502M_10196.pdf?sequence=1. 21 Dec 2018.
International Association of Professional Security Consultants/ IAPSC. (2015). Detention of shoplifting suspects by loss prevention and security personnel. Available at: https://iapsc.org/wp-content/uploads/2015/08/BestPractices_Shoplifting.pdf. 29 July 2018.
Jack L. Hayes International, Inc. (2018). 30th Annual Retail Theft Survey, Press release. Accessed at: http://hayesinternational.com/wp-content/uploads/2018/05/30th-Annual-Retail-Theft-Survey-WithThoughts-1.pdf. 24 Nov 2018.
Karpp, D. (2017). The 2017 Hiscox Embezzlement study: A report on white collar crime in America. Accessed at: https://www.hiscox.com/documents/2017-Hiscox-Embezzlement-Study.pdf. 23 Nov 2018.
Kennedy, J. P. (2017). Functional redundancy as a response to employee theft within small businesses. *Security Journal, 30*(1), 162–183.
Martin, T., Hollinger, R., Laskey, H. O. Jr., Smith, A., & Deyle, E. (2014). Employee theft: Statistics, interviewing techniques, and tips to optimize your employee theft policy. LPM Special Report. Accessed at: https://losspreventionmedia.com/free-reports/employee-theft-statistics-interviewing-techniques-and-tips-to-optimize-your-employee-theft-policy/. 23 Nov 2018.
Mishra, B. K., & Prasad, A. (2006). Minimizing retail shrinkage due to employee theft. *International Journal of Retail & Distribution Management, 34*(11), 817–832.
Moorthy, M. K., Seetharaman, A., Jaffar, N., & Foong, Y. P. (2015). Employee perceptions of workplace theft behavior: A study among supermarket retail employees in Malaysia. *Ethics & Behavior, 25*(1), 61–85.
Moraca, R., & Hollinger, R. C. (2018). *2018 National Retail Security Survey*. National Retail Federation. Accessed at: https://cdn.nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf?_ga=2.160184253.1479417109.1543004597-1296545894.1530641166. 23 Nov 2018.
Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.
Nemeth, C. P. (2019). *Private security and the investigative process* (4th ed.). Boca Raton: CRC Press.
Peltier-Rivest, D., & Lanoue, N. (2011). Thieves from within: Occupational fraud in Canada. *Journal of Financial Crime, 19*(1), 54–64. https://doi.org/10.1108/135907912111907

Further Reading

1. Brady, M. K., Vorhees, C. M., & Brusco, M. J. (2012). Service sweethearting: Its antecedents and customer consequences. *Journal of Marketing, 76*(2), 81–98.
2. Hayes, R. (2007). Employee deviance. In *Retail security and loss prevention* (pp. 3–16). London: Palgrave Macmillan.
3. Kennedy, J. P. (2016). Sharing the keys to the kingdom: Responding to employee theft by empowering employees to be guardians, place managers, and handlers. *Journal of Crime and Justice, 39*(4), 512–527.
4. Lyons, B. D., & Bowling, N. A. (2017). On the effectiveness of peer reporting policies. *Journal of Managerial Psychology, 32*(8), 547–560.

Retail Security: Shoplifting

Lauren R. Shapiro
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Inventory shrinkage · Shop theft · External retail crime · Loss prevention and asset protection · Adult and adolescent shoplifters

Definition

The Federal Bureau of Investigation (FBI 2016a) categorizes shoplifting in the Uniform Crime Reporting (UCR) as larceny-theft under property crime offenses, defined as "unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another." Retail shoplifting refers to "the theft of goods by customers from retail premises during opening hours" (Wittenberg 2009, as cited in Hirtenlehner et al. 2014, p. 14).

Introduction

Retail stores sell a variety of goods (e.g., clothes, food, drugs, music, candy) for public consumption and use. Inventory shrinkage is a serious problem for retailers globally, with external theft/shoplifting in 2017 accounting for 37% of the $49 billion in economic loss for the retail industry in the USA alone (National Association for Shoplifting

Prevention [NASP] 2014a; Moraca and Hollinger 2017). Although alarming, this statistic actually represents a reduction from shoplifting incidents, one of the largest sources of shrink, which was 39% in 2016 and 38% in 2015 (NASP 2014a). NASP (2014a) reported that other sources of shrink stemmed from internal/employee theft (30%), administrative error (21%), vender fraud/error (5%), and unknown (7%).

Even more disconcerting, only 10 million shoplifters out of an estimated 27 million shoplifters in the United States over a 5-year span had been caught (NASP 2014a). Juveniles comprise one-fourth of shoplifters and adults comprise the rest (NASP 2014a). Larceny-theft encompassed 71% of all property crime offenses in 2016 (FBI 2016a). Shoplifting offenses affect every region of the USA, comprising 24% of larceny-theft offences in the Northeast, 23% in the Midwest, 22% in the South, and 22% in the West (FBI 2015). To combat inventory shrinkage from shoplifting, many retailers rely on the services of private security/loss prevention personnel (see ▶ "Retail Security: Use of Security Guards" chapter and ▶ "Security Guards: Authority and Power" chapter in this volume), loss prevention awareness and training, and antitheft devices (Moraca and Hollinger 2017). This chapter focuses on describing shoplifter demographics, motives, and methods, as well as legal responses for retailers and loss prevention agents who apprehend shoplifters.

Shoplifter Demographics

Retailers and their agents (e.g., clerks, private security officers, loss prevention personnel) attempt to differentiate potential and active shoplifters from nonoffending customers and to apprehend them during or subsequent to the commission of their crime. The most common strategy used is offender profiling, which relies on the typical demographics of offenders described in law enforcement apprehension reports (Shapiro and Maras 2017). Official arrest data indicate various characteristics, such as sex, age, and race/ethnicity, of those arrested for larceny theft. Shoplifting, however, is but one type of larceny theft, so the statistics reported include those arrested for other larceny-theft offenses (e.g., pick pocketing, purse snatching, bicycle theft), as long as stealing was not done by force or violence (FBI 2015).

The majority of juvenile and adult offenders arrested for larceny-theft offenses (57%) have been male (FBI 2015). According to the FBI (2016a, 2016b), juveniles were responsible for 13% of property crime offenses (6% at ages 10 to 12; 21% at ages 13 and 14; 20% at age 15; 25% at age 16; 28% at age 17) and adults 18 years and older (7% for ages 18–19; 18% for ages 20–24; 17% for ages 25–29; 14% for ages 30–34; 8% for ages 40–44; 7% for ages 45–49; 5% for ages 50–54; 4% for ages 55–59; 3% for ages 60 and up) were responsible for the remaining 87%. Race/ethnicity data indicated that the majority of juvenile larceny-theft offenders were European American (60%, only 13% identified as Latina/o), 36% were African American, 1.6% were Asian American, and 2% were from Native/Pacific Islander American (FBI 2016a). Similarly, adult larceny-theft offenders were predominantly European American (70%, only 14% identified as Latina/o), 27% were African American, 1% were Asian American, and 2% were from Native/Pacific Islander American (FBI 2016a). In summary, the demographic profile for larceny-theft offenders would be predominantly male and European American; as for age, juvenile offenders would likely be 15–17 years old, whereas adult offenders would likely be 20–34 years old.

Does this profile accurately represent shoplifters? The answer is probably not; if it did, there would be a high apprehension rate and low shrink rate from shoplifting. There are several problems with the database itself. Most importantly, the arrest dataset is too broad in that it is comprised of all larceny theft offenders and is unlikely to be a true representation of all shoplifters. As previously mentioned, the majority of shoplifters are simply not detected by retailers. Shoplifters steal on average between 48 and 150 times before being apprehended (Farrington 1999; Harnischmacher 2000, as cited in Hirtenlehner et al. 2014; NASP 2014a; Nelson and Perrone 2000; Williams et al. 1987).

Also missing from the arrest data are shoplifters apprehended by retailers who are not turned over to the police. Even when stores post a "notice of intent to prosecute shoplifting" sign, fewer than one-fourth of them are arrested and formally charged (Elliott 1995). According to Moraca and Hollinger (2017), the average number of shoplifter apprehensions declined from 3455 in 2015 to 3323 in 2016 to 1441 in 2017, despite a significant increase in the rate of shoplifting, which averaged a loss of $798.48 per incident in 2017 ($974 per incident for apparel).

The arrest data are also distorted (i.e., not inclusive of all apprehended shoplifters) due to police officers' use of discretion, which allows them not to charge some offenders (e.g., because of age, criminal history, merchandise cost); instead, offenders are released with a warning, resulting in only a small proportion of all shoplifters who are actually booked (Dabney et al. 2004). Further, the average number of shoplifting cases prosecuted has declined over a 3-year period from 2739 in 2015 to 1935 in 2016 to 742 in 2017 (Moraca and Hollinger 2017). Researchers estimate that 1/5 to 1/3 of shoplifting offenders are not included in the FBI system (e.g., fingerprints) nor charged with each index offense, often leading to increased differences in recorded demographics, particularly for race and age (Elliott 1995).

Official arrest statistics are also a reflection of societal stereotypes and prejudices in regard to the typical criminal. These biases affect the retailers and their agents' decisions of whom to surveille, typically those who fit the physical appearance of a "criminal" stereotype (i.e., male, African-American, lower-class) profile, and whether or not the shoplifter gets processed, charged, and sentenced in the criminal justice system (Dabney et al. 2004; Shapiro and Maras 2017). In this way, the official profile is reinforced, despite the fact that shrink continues to increase. By limiting their scope, retailers are actually allowing shoplifters who do not fit the stereotype to steal without threat of apprehension (Shapiro and Maras 2017). The impact of stereotypes becomes apparent when retailers and their agents target potential shoplifters from groups that are out-of-sync with their representation in the population. Differential surveillance practices due to consumer racial profiling result in a higher number of African American shoplifters being arrested than are actually represented in the population (Dabney et al. 2004). The result is often harmful to the reputation of the store, reduction in minority shoppers, and lawsuits, without effectively reducing shoplifting incident rates (Shapiro and Maras 2017).

To understand who the shoplifter really is, retailers must consider information from a number of sources. Research findings examining the public's criminal stereotypes have been mixed, as some believed shoplifters to be usually female (Dabney et al. 2004) and others usually male (Shapiro and Maras 2017). Self-report data indicated that boys/men and girls/women from a variety of ethnic/racial backgrounds shoplifted equally (Elliott 1995; NASP 2014a). However, the official rate of 57% of men that were arrested for larceny-theft (FBI 2015) was suspicious as it was higher than their representation in the population, which according to the 2016 US Consensus was estimated as 49% (Pew Research Center 2018). Similarly, arrest and imprisonment of juvenile and adult minority offenders for larceny, particularly African Americans (36% and 27%, respectively) and Native/Pacific Islander Americans (2%, each), demonstrate disproportionate treatment in comparison to their representation in the population. According to the US Census for 2016, estimated proportions of citizens were 13% African American descent and 0.8% Native American/Pacific Islander American (Pew Research Center 2018). In summary, given the spontaneity of shoplifting incidents, the proportions of sex, age, and ethnicity/race should reflect the population in that area and region of the country. To best understand the common demographics of the common shoplifter for their stores, retailers must examine the demographics of their customer base, allowing for the probability that anyone may shoplift.

Motives of Shoplifters

The majority of children (72%) and adults (73%) who shoplifted indicated that they did so spontaneously (Gold and Lang 2012; NASP 2014a).

Shoplifters have a variety of motives for stealing, but the perception that the act is low risk facilitates and maintains the behavior (Tonglet 2002). Both juvenile and adult shoplifters steal for financial reasons, obtaining items that they could not otherwise afford, usually luxury products rather than basic necessities. Some shoplifters are involved in organized criminal gangs and their "job" is to steal a list of items for the sole purpose of resale or profit (NASP 2014a). Peer pressure is another motivation, particularly for youth who may be required to show they can be brave or loyal to their friends or gangs. Another motive is emotional (NASP 2014a), particularly when shoplifters receive an emotional boost or thrill from successfully stealing (i.e., obtaining merchandise without getting caught by loss prevention agents). Others engage in shoplifting to support their substance abuse addictions or because they have psychological or mental health disorders, such as depression or kleptomania, an impulse disorder (NASP 2014c). Even when caught, shoplifters may engage in rationalization and neutralization to reduce their moral responsibility for the crime (Cromwell and Thurman 2003).

Typical Methods for Shoplifting

Retail and loss prevention personnel should learn which behaviors are typically exhibited by shoplifters as a means for discerning them from shoppers. Specifically, juveniles and adults who intend to steal will often exhibit signs of nervousness (e.g., facial grimaces, eye darting, lip and/or nail biting, shoulder tension), pick up merchandise, then look around to determine the location of cameras and staff, and bring items to remote areas of the store (Dabney et al. 2004). They choose busy, peak times to commit their theft knowing that it is more difficult for clerks to detect them or distinguish them from shoppers. Shoplifters may even purchase some items to avoid suspicion or, if caught, to appear to be the "absent-minded" shopper.

There are three main methods – concealment, grab-and-escape, and price/electronic tag tampering – used by shoplifters to steal items. Shoplifters commonly use concealment as their means to steal (Dabney et al. 2004). Potential shoplifters will enter stores with empty bags, containers, and even strollers or wear bulky clothing that may even be out of sync with the weather, all of which can be used to hide merchandise (Dabney et al. 2004). Although shoplifters do work alone, more often they work in pairs or groups. One member serves as a distracter, engaging the sales staff in various ways such as requesting they retrieve an item from the back of the store or by asking questions, while the other member or members steal merchandise on the sales floor or by taking it inside the dressing room where they conceal it within another container, such as a bag, or on themselves, such as under their clothes or coat (Dabney et al. 2004). Shoplifters may be accompanied by young children who serve as a distractor or whose strollers or carriages provide an area to conceal items. This technique provides plausible deniability for shoplifter-parents as they can blame the child for taking the items or indicate that they placed items inside while caring for the child and then forgot about them. Another method, grab-and-escape, involves a person or a group of people rushing in, grabbing one or more items, and then running out of the door. Stealing is also accomplished by switching high price tags with low prices tags, removing electronic tags, and/or by returning stolen items for a refund. According to Moraca and Hollinger (2017), fraudulent returns averaged $1766 for all retail ($969 for retail apparel).

Retailer Responses to Shoplifting Within the Law

The states allow retailers and their agents who have "probable" or "reasonable" cause to invoke "merchant's privilege" to detain a suspected shoplifter (International Association of Professional Security Consultants/IAPSC 2015, pp. 2–3; Nemeth 2018, p. 187; also see ▶ "Investigations: Criminal" chapter in this volume). Consistent with the definition of retail theft offense, the agent must witness the suspect approach merchandise offered for sale, stored, or on display;

take it (i.e., be in possession of it); and intentionally deprive the owner of it by (willfully) carrying it away, concealing it, converting it, or failing to pay for it (IAPSC 2015, p. 3; Nemeth 2018, p. 171; see also ▶ "Investigations: Consumer Retail Shoplifting" in this volume). Conversion is the process of retail theft by which a person alters the price of merchandise or renders the inventory control tag on it inoperable by destruction or removal (Nemeth 2018, p. 171).

Agents must have firsthand knowledge for misdemeanor offenses (i.e., directly observe) and reasonable grounds for felony offenses that the suspect took and failed to pay for the merchandise (Nemeth 2018, p. 188). An agent may make a "citizen's arrest" – but only if the agent witnessed a misdemeanor crime or when the agent is informed and is certain that a felony crime occurred (Nemeth 2018, p. 187). Agents should identify themselves upon approach of the suspect and present credentials while acting in a professional and calm manner. Most states allow agents to detain the suspect upon concealment of the unpurchased merchandise, whereas some states require that the suspect leave the store (IAPSC 2015). In the latter case, the suspect should be asked to return the merchandise and then accompany the agent back to the store (IAPSC 2015). When processing suspects, agents should ensure their safety from hidden weapons by separating suspects from their bags and, when necessary, perform a "Terry-style" pat-down (Nemeth 2018, p. 187).

There is limited civil liability protection when a suspect is detained for a limited amount of time by an agent who has a reasonable suspicion of shoplifting in order to investigate the merchandise theft, recover it, and summon the police (Budden 1999; IAPSC 2015, p. 4). These "Merchant statutes" allow agents to search for unpaid merchandise inside suspects' possessions, such as their bags or baby strollers, but does not allow them to conduct a search of the person's body or clothing (Budden 1999). A best practice approach is recommended to reduce the likelihood of successful civil liability suits against the retailer and agents (IAPSC 2015). According to IAPSC (2015), the agent should: (a) approach and use nonthreatening language and actions towards the suspected shoplifters; and (b) avoid physical handling of the suspect, limiting use to minimal force only for restraining someone from fleeing, except when bystanders are nearby or when against store policy (i.e., no touch, no chase), in which case agents should call the police. Even when the police are not involved, it is important that agents make an in-house loss prevention report that provides important information regarding the shoplifter's demographics, itemizes the stolen items and costs, identifies witnesses, and includes a narrative of what happened. Stolen merchandise should be photographed, logged, and stored for evidence if a court case is made or, if allowed, restocked.

After confirming that the suspect did indeed steal items from the store, retailers must decide whether to handle the shoplifting incident informally (aka catch-and-release), such as talking to the parents or through in-store sanctions (e.g., trespass agreement), or formally by turning the shoplifter over to the police or file civil damages (Gold and Lang 2012; NASP 2014b). The decision to process individual shoplifters formally by contacting the police for subsequent arrest and prosecution is a difficult one; retailers call the police for about half of all apprehensions, even though warnings of prosecution signs have been posted (NASP 2014a; Williams et al. 1987). Alternatively, retailers may use civil recovery by suing the offender for loss and damage of merchandise (Gold and Lang 2012). In contrast, shoplifters who part of an organized shop theft group, that is, those who have a list with items to be stolen that match the shoplifted items, should be turned over to police (Martinez 2005).

Retailers may seek compensation for expenses associated with the shoplifting incident and penalty damages, regardless of whether the items stolen were recovered undamaged (NASP 2014b). Ideally, retailers would prefer to eliminate or severely reduce shoplifting and the costs associated with it. A Canadian study in British Columbia showed that recidivism up to 2-years later was lower among shoplifters who completed a community-based restorative justice program supported by federal government funding than

those processed through the criminal justice system (e.g., Robinson et al. 2013). Of particular interest was recidivism for shoplifters with criminal histories: 70% of adult women and 88% of adult men who were charged reoffended versus 29% of women and 50% of men who completed the restorative justice program reoffended. There are restorative justice-themed diversion programs associated with American courts at public expense but only about one-fourth of them track recidivism as an indicator of success (Gold and Lang 2012).

Beginning in 2011, merchants in the United States (e.g., Walmart, DSW, Bloomingdales, Burlington, Decathlon, Kroger) offered offenders the choice of arrest or to pay for a shoplifting restorative justice education course, such as one offered and administered by Corrective Education Company, aimed at reducing recidivism (Rappaport forthcoming; Richey 2016). The benefits were threefold as retailers were not financially responsible for the course fee and did not have to contact and provide evidence to law enforcement; offenders were kept out of the criminal justice system; and the community did not have to pay police and court fees associated with shoplifting offenses (Rappaport 2018). However, the recidivism rates were less clear as only the for-profit agency evaluated the data. This company was involved in a recent summary judgment, *People v. Corrective Education Company* et al. (2017), in which the Court ruled that forcing shoplifters to watch the video of the restorative justice program and then to choose between criminal prosecution or paying for the program amounted to false imprisonment and extortion. In the wake of this decision, a RICO class action law suit was filed on April of 2018 with the Supreme Court (see Doe et al., v. Walmart Inc. 2018).

Conclusion

Retail shoplifting has a dramatic impact financially on society in a variety of ways. Clearly, the businesses that lose revenue through shoplifting are directly affected. However, there is an indirect, domino effect caused by shoplifting when retailers are forced to hire loss prevention staff and purchase antitheft security devices. Specifically, employees are laid off or have their wages reduced in order for companies to recover the cost of deterrence measures and make up for the loss of potential income and profit. Consumers are dually burdened by the increase in the cost of items and the inconvenience that the loss prevention techniques provide for shopping (Richey 2016). Additionally, local jurisdictions must absorb the cost of increasing law enforcement to arrest shoplifters and paying associated expenses from court cases for prosecutors to charge the shoplifters and for judges to hear the cases (NASP 2014a). Communities lose important revenue though commercial taxes on the items that were stolen instead of being purchased and on income taxes from stores when retailers move out of the neighborhood due to the high losses suffered from shoplifting (NASP 2014a). Store closings, in turn, increase unemployment for those in the affected areas, as well as impact the economic well-being of the nation.

Cross-References

- ▶ Arrest
- ▶ Investigations: Consumer Retail Shoplifting
- ▶ Investigations: Criminal
- ▶ Retail Security: Use of Security Guards
- ▶ Security Guards: Authority and Power

References

Budden, M. C. (1999). *Preventing shoplifting without being sued: Practical advice for retail executives*. Westport: Quorum Books.

Cromwell, P., & Thurman, Q. (2003). The devil made me do it: Use of neutralizations by shoplifters. *Deviant Behavior, 24*(6), 535–550.

Dabney, D. A., Hollinger, R. C., & Dugan, L. (2004). Who actually steals? A study of covertly observed shoplifters. *Justice Quarterly, 21*(4), 693–728.

Doe et al., v. Walmart Inc. et al. (2018). No. 5–18-cv-02125 (N.D. Cal.).

Elliott, D. S. (1995). *Lies, damn lies, and arrest statistics*. The Sutherland Award Presentation at the American Society of Criminology meeting, Boston. Available at https://www.colorado.edu/cspv/publications/papers/CSPV-015.pdf. 5 July 2018.

Farrington, D. P. (1999). Measuring, explaining, and preventing shoplifting: A review of British research. *Security Journal, 12*, 9–27.
Federal Bureau of Investigation. (2015). 2015 crime in the United States. U.S. Department of Justice. Available at https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-42. 5 July 2018.
Federal Bureau of Investigation. (2016a). 2016 crime in the United States. U.S. Department of Justice. Available at https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/larceny-theft. 5 July 2018.
Federal Bureau of Investigation. (2016b). 2016 crime in the United States. U.S. Department of Justice. Available at https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/tables/table-20. 22 July 2018.
Gold, E., & Lang, J. (2012). Diverting shoplifters: A research report and planning guide. Center for Court Innovation. Available at https://ric-zai-inc.com/Publications/cops-p227-pub.pdf. 29 July 2018.
Hirtenlehner, H., Leitgob, H., & Birklbauer, A. (2014). Juvenile shoplifting delinquency. Findings from an Austrian study. *SIAK-Journal: Journal for Police Science and Practice (International Edition), 4*, 14–29. https://doi.org/10.7396/IE_2014_B.
International Association of Professional Security Consultants. (2015). Detention of shoplifting suspects by loss prevention and security personnel. Available at https://iapsc.org/wp-content/uploads/2015/08/BestPractices_Shoplifting.pdf. 29 July 2018.
Martinez, L. (2005). Combating organized retail theft in 2005. *Security Technology and Design, 15*(2), 58.
Moraca, R., & Hollinger, R. C. (2017). 2017 National retail security survey. Available at https://nrf.com/system/tdf/Documents/NRSS-Industry-Research-Survey-2017.pdf?file=1&title=National%20Retail%20Security%20Survey%202017
National Association for Shoplifting Prevention. (2014a). Shoplifting statistics. Available at http://www.shopliftingprevention.org/what-we-do/learning-resource-center/statistics. 22 July 2018.
National Association for Shoplifting Prevention. (2014b). Shoplifting and civil law. Available at http://www.shopliftingprevention.org/what-we-do/learning-resource-center/shoplifting-and-civil-law. 22 July 2018.
National Association for Shoplifting Prevention. (2014c). Psychological studies on shoplifting and kleptomania. Available at http://www.shopliftingprevention.org/what-we-do/learning-resource-center/psychological-studies. 22 July 2018.
Nelson, D., & Perrone, S. (2000). Understanding and controlling retail theft. *Trends & Issues in Crime and Criminal Justice, 152*, 1–6 Accessed 7 Nov 2016 at http://search.proquest.com.ez.lib.jjay.cuny.edu/docview/189475073?rfr_id=info%3Axri%2Fsid%3Aprimo.
Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.
People of the State of California v. Corrective Education Company. et al. (San Francisco Superior Court Case No. CGC-15-549094, Filed August 14, 2017; Filed originally Nov. 23, 2015, Cal. Ct. App. Filed April. 13, 2017).
Pew Center Research. (2018). 2016 American Community Survey 1-year estimates. U.S. Census Fact Finder: American Community Survey. Accessed at https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_16_1YR_CP05&prodType=table. 19 Feb 2018.
Rappaport, J. (2018). Criminal justice, Inc. University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 818; University of Chicago, Public law working paper no. 641. *Columbia Law Review, 118*. Available at SSRN: https://ssrn.com/abstract=3059793 or https://doi.org/10.2139/ssrn.3059793
Richey, D. (2016). Walmart's 'second chance' plan. *Security, 53*(11), 10.
Robinson, K., Plecas, D., Squires, C., & McLandress, K. (2013). *The impact of restorative justice on recidivism among shoplifters*. Abbotsford: Centre for Public Safety and Criminal Justice Research Accessed 29 July 2018 at https://www.correctiveeducation.com/home/uploads/Restorative-Justice-Report.pdf.
Shapiro, L. R., & Maras, M.-H. (2017). Stereotypes affect surveillance. *Security Management, 61*(4), 44–49.
Tonglet, M. (2002). Consumer misbehavior: An exploratory study of shoplifting. *Journal of Consumer Behavior, 1*(4), 336–354.
Williams, H., Forst, B., & Hamilton, E. E. (1987). Stop: Should you arrest that person? *Security Management, 31*(9), 52–58.

Furthur Reading

Christman, J. H., & Sennewald, C. A. (2006). *Shoplifting: Managing the problem*. Alexandria: ASIS International.
Nemeth, C. P. (2019). *Private security and the investigative process* (4th ed.). Boca Raton: CRC Press. [see Retail Theft chapter].
Sennewald, C. A., & Christman, J. H. (2008). *Retail crime, security, and loss prevention an encyclopedic reference*. Burlington: Elsevier.

Retail Security: Use of Security Guards

Kenneth J. Grossberger
John Jay College of Criminal Justice, New York, NY, USA

Keywords
Security guard · Loss prevention · Shrinkage · Shoplifting · Organized retail crime (ORC)

Definition

Retail security is the protection of goods, personnel, and customers in the exchange of those assets in a store setting, a shopping mall, online, and in locations in the chain of supply that provides those goods and services.

Introduction

Security guards are a key protective component for the US retail industry, which had gross sales of about $3.8 trillion in 2019 (Young 2020; Digital 360 Commerce 2020). Security guards protect stores, malls, warehouses, and distributions centers, and they also control access, provide visible deterrence, protect customers and store staff, protect assets, conduct investigations, perform customer service tasks, and assist store management. Retail establishments have been using guards as a primary form of security for many years.

The Purpose of Retail Security

The two basic functions of retail security are loss prevention (LP) and safety. Security guards are responsible for both. Loss prevention is synonymous with asset protection (LP Magazine 2020), and retail security personnel are sometimes called asset protection officers or loss prevention specialists, depending on the assignment.

Loss Prevention

Loss prevention is a general term for controlling any kind of loss in a retail establishment (LP Magazine 2020). This also involves asset protection, which includes merchandise and products (the inventory), the store equipment and logistics, the computer and communication equipment, and the displays.

Safety

Security officers are also responsible for the safety of shoppers and staff and perform patrols and inspections in stores and other retail facilities. They also perform safety functions such as evacuations and fire drills.

Physical Security

The primary responsibility for retail security guards is to protect the stores. In addition, guards protect retail facilities such as malls, warehouses, and distribution centers. Guards are sometimes responsible for retail inventory, stock, deliveries, and transportation of retail goods. Physical security includes staff well-being, brand risk, and physical damage to retail facilities (Humphreys 2019).

Store Models

There are several different models of stores, and each presents different risks and challenges for security guards. There are numerous clothing stores including chain stores and individual local stores. There are also chain supermarkets, jewelry stores, pharmacies, "specialty" (stores that sell a variety of goods), department stores, drug stores, convenience stores, and discount stores (Bhasin 2018). Stores may be in outdoor malls, indoor malls, strip malls, commercial office buildings, commercial office parks city streets, and piers.

Security Guard Responsibilities and Posts

As in other venues, a security officer on post at a retail location is responsible for the basic functions of observe and report, post and patrol, as well as customer service (Spadanuta 2010; Purpura 2002). In addition, a guard acts as a visible deterrent against crime, including shoplifters and other would-be offenders (Dempsey 2010).

There are other security assignments in retail environments such as a loss prevention specialists who perform the basic security functions but who also may have responsibility for inventory (deliveries, counts, controls, and reporting), incident investigations, shoplifting, burglary, fire prevention, safety, organized retail crime (ORC, see below), coordination with mall or building security, and security incident statistics (Purpura 2002). Store detectives (SDs) patrol the interior of stores and make apprehensions if they spot

shoplifters and ORC boosters. Some other security guard responsibilities are to act as an undercover (UC), plain clothes agents (who usually do not make apprehensions as their mission is to report theft, fraud, and other illicit behavior), and to be responsible for such concerns as sweethearting (see below), inventory issues, credit card fraud, and other negative activity when observed. UCs remain anonymous because their exposure would minimize their effectiveness. Their reports go to senior retail company management for further action. Security personnel in retail locations are usually unarmed because the billing rates are cheaper and there is less liability. Armed posts are used in high crime areas and where there is money or other critical assets to be protected. Armed personnel are also used for events in stores where celebrities or models are present.

Post Orders and Uniforms

Post orders are an industry standard and are used as specific orders and instructions for security personnel on post and "are written instructions of activities that security officers are expected to perform and should be detailed and reflect expectations" (Seivold 2019). This may include the use of logbooks (paper and electronic) and how to make entries, methods of checking in and out, reporting incidents, attire and grooming, customer service standards, and emergencies procedures (including evacuation instructions).

Security personnel may wear a number of different kinds of uniforms. While the police style uniform was the standard for many years, more recently, public-facing retail establishments have been using soft look uniforms such as blazers and slacks with white shirts and ties. Security officers may wear patches on the blazers or have a security pin on their jacket pockets to identify as security. UCs, store detectives, and supervisors are usually in plainclothes so as to blend in with shoppers and hide their identities.

Security Personnel Management and Supervision

The management and supervision of security personnel in the retail environment is critical to the success of any security/safety program. Guards and other officers must be properly hired and vetted. For example, guards must be checked by means of the following: security license checks and fingerprinting, criminal records check, previous employment verification, background checks, drug tests, driving record checks, social security number verifications, proof of legal right to work, federal and state criminal record checks (pursuant to state requirements), personal reference checks, education verification, military service verification, and previous employment verification (Secure Community Network n.d.).

Officers must be trained in the following areas: entry security, observation techniques, shoplifting, ORC (see below), customer service, incident deescalation, emergency procedures, evacuations, the role and purpose of private security, professional attitude, communication skills, proper recording and reporting of events and incidents, civil liability, violation of policy and procedure, workplace diversity, and sexual harassment issues. Officers must also receive post-specific instructions. The purpose of training is to ensure the guard has "observable and measurable knowledge, skills, abilities, and personal attributes that contribute to enhanced employee performance and ultimately result in organizational success" (Kitteringham 2020).

Most US states have licensing requirements for security (SecurityGuard-License.org n.d.), and if unlicensed personnel are deployed, the potential liability is significant for both the security company and the retailer. For example, if there is an incident and the retailer is sued, the security company's general liability insurance policy covers this risk, but if the officer involved is not licensed, the insurance company may disclaim liability leaving both the security company and the retailer unprotected.

Security officers take several tests during their careers, and there are almost always state-mandated tests as part of the licensing process (SecurityGuard-License.org n.d.). Retests are usually taken upon license renewal. Officers, typically, have to take tests as part of the hiring process as well to see if they have sufficient knowledge to be a security officer. If there is

additional training, say for ORC or emergency procedures, there may be testing for these areas as well. If retail locations require professional certifications, for example, automatic external defibrillators and cardio-pulmonary resuscitation (AED/CPR), first aid, blood-borne pathogens, or fire guard, then that training requires testing as well (American Red Cross n.d.).

Similarly, supervising security personnel on duty at retail locations require industry knowledge and experience to support the officer and ensure that the store's post instructions are being followed. Security supervisors are on the ground, in retail locations, and face to face with security officers and customers. Their responsibilities are to the officer, the company they work for, or the store if there are proprietary personnel. Field supervisors are usually uniformed in such a way as to be identifiable as security, and may wear badges, patches, or pins to indicate this. Supervisors are response for "hiring, training, discipline, motivation, promoting and communicating" with security guards (Sennewald 2003).

Contract Versus Proprietary Security Guards

There are different models for security in retail, and the most significant is whether personnel are contract security (security companies) or proprietary security (in-house). Contract security guard sales were about $31 billion in 2018 (Mazareanu 2019), and such services were widely used. The security industry has many companies that provide security services to stores, malls, warehouses, and distribution centers. The larger retail companies with chain stores may have their own LP (or asset protection) departments, made up of executives, directors, regional managers, loss prevention investigators, and specialty personnel (such as ORC investigators or undercover agents). The responsibility is the same, whether a store uses contract security or its own personnel, and in many cases, stores used a mixed model with both contract security and their own asset protection staff. The LP departments for retail companies typically hire contract security personnel for entry security, interior patrol, store detective assignments, and loss prevention specialists, while proprietary staff handle management and specialty assignments. The main reasons for using contact security are that it is usually less expensive and security companies provide insurance coverage for the retail company. The client (the retail company) becomes an "additional insured" on the security company's general liability policy, meaning that the security company's insurance company accepts the liability of the client (Kagan 2020). These are strong incentives to use contract security as opposed to in-house personnel. The decision to spend money on contract security depends on shrinkage, store sales, and other risk factors. For example, if a store has high shrinkage but high sales, there is the need and the budget to hire contract security. But if store sales are low, the management's decision may be to not hire security even of the shrinkage is high. There may be risk factors that increase the need for security guards such as crime in the mall or the surrounding area. Guards are often hired to provide protection for store employees.

Mall security typically does not have responsibility for security in the stores themselves due to the liability of acting in a leased area where mall security is not specifically allowed, and also because there may be store proprietary guards on site (especially for chain stores) that is contracted for the security function. Conversely, store security typically has no responsibility for the mall areas as an officer assigned to a store must protect that venue and not leave the store if there is a problem somewhere else in the mall. However, store security often works with mall security on evacuations, events (e.g., holidays), and if security incidents occur (e.g., sharing of evidence, interviewing witnesses). There are many such opportunities for store security to interact with mall security.

Inventory and Shrinkage

Inventory is defined as "goods available for sale and raw materials used to produce goods available for sale" (Kenton 2019). Inventory represents the most important asset to be secured and also presents the greatest risk in retail security. Protection is required as the "turnover of inventory represents one of the primary sources of revenue generation" (Kenton 2019).

Shrinkage is defined as the difference between inventory and what got sold, or "loss of inventory related to theft, shoplifting, error, or fraud" (McCue 2019). In addition, there may be internal theft, damaged garments, credit card and gift card fraud, missed markdowns, or other inventory issues. Missed markdowns occur when goods that were reduced in price for a period of time are not increased back to the original price. Such errors cost the nongrocery retail industry over $300 billion in 2018 and were due, in part, to "inventory misjudgments" (Garcia 2019). In stores that sell equipment, there might be damage or vandalism (rendering it unsaleable). In food stores, there may be spillage, spoilage, and product being eaten (both by shoppers and staff), which reduce sales. Another factor is a store associate's employee discount abuse, where some shoppers get a break in the price due to an error, sweethearting (see below), or theft for payoff (e.g., a shopper gets a $20 price reduction and gives $10 back to the associate).

A major risk factor in assessing shrinkage is the cashiers at checkout. Even with all the technology such as electronic cash registers, CCTV systems, data systems that monitor cash and credit sales and Exception Based Reporting (or EBR, which finds "exceptions" to the normal patterns of sales so that LP personnel can focus on potential fraud and is defined as "a method of data analysis that compares an incoming stream of data to an established base set of data and flags items that don't quite match up," EBR-Group.net n.d.), the point of sale (POS) is still one of the biggest liabilities for a retail establishment. There is a great deal for a cashier to do: check out the merchandise, take the payment (cash, credit/debit card, gift card, store card, and credit voucher), process an exchange of items, answer customers' questions, and watch for shoplifting (Resume Resource n.d.). One risk in stores where shopping carts are used is to miss items in the "bottom of the basket" (BOB) which results in an unpaid merchandise (Progressive Grocer 2006). Store security can assist cashiers at high volume times and watch for these risks, or deter them, and UCs can check cashiers and report theft and fraud. All these factors contribute to shrinkage. There are other transactions that contribute to shrinkage such as credit card fraud (a federal offense), gift card scams (the use of phony gift cards supposedly issued by the store), price tag switching, and return item fraud (trying to return an item for credit that was not purchased) (Sennewald and Christman 2008).

Security guards, loss prevention specialists, UCs, and store detectives have a direct effect on reducing shrinkage. By effectively controlling store entry, observing store staff, patrolling the store, using security technology, making apprehensions, and using other techniques, store security may deter theft and reduce losses.

The retail industry annual shrink rate was 1.38% in 2018 (National Retail Federation 2020), which is comparable for previous years. But, that amounts to losses of over $52 billion. While there is a variety of technical means to reduce shrinkage, security guards and other forms of organic security are primary defenses in the protection of retail establishments. Internal losses in a store (including employee theft, inventory issues, and product damage) account for about 60% of the total (McCue 2019). Other losses come from shoplifting, ORC (see below), chain of supply issues (see below), and other factors (McCue 2019). The calculus by industry executives takes these data into account when considering budgets for security guards and other loss prevention personnel.

Theft Techniques

Shoplifting

One of the key factors in store loses is shoplifting, which comes in several forms from amateurs to professionals (Purpura 2002). There are shoplifters who shoplift often, the frequent flyers, either as a means of supplementing their income or to get free goods. There are the so-called casual shoplifters, who steal items occasionally in order to create their own discounts. Then there is the once in a lifetime shoplifter, who never stole anything before. The professional shoplifters may work in teams or alone but are associated with criminal organizations, and this falls under the

heading of organized retails crime (ORC), more on this below. Security uses the techniques mentioned above for deterring, spotting, and apprehending shoplifters. The means by which shoplifting is dealt with depends on store policy as some retailers are more aggressive about security (apprehensions) and others are more concerned with the guest experience and are less inclined to confront thieves in order to avoid physical incidents in the store that might disturb patrons.

Sweethearting

Sweethearting is a technique used by thieves to compromise a member of the sales team or the cashier. This is done by the thief being friendly to the team member in order to get a discount get something for free, or to distract that team member while an associate steals something (Hollinger 2018). UCs and LP personnel can spot such activity and deter it or make apprehensions as needed, and in accordance with the post orders.

The Robin Hood Effect

One source of loss occurs when employees try to help patrons they think are in need. This comes in the form of free or discounted merchandise, extended sales, or military or specialty discounts extended to nonqualifying shoppers. While these actions come from "good intentions and a desire to help others," they have a "significant impact on the bottom-line" (Penizotto 2020). A loss prevention specialist may be charged with the responsibility to monitor or stop this behavior or report it as dictated by store policy. The effect, coming from the perception of taking from the rich and giving to the poor, is that the behavior is justified as the company has a lot of money and the shopper is needy (Penizotto 2020). Undercover agents can be trained to spot this activity and to report it as necessary.

Organized Retail Crime

Organized retail crime (ORC) "involves the large-scale theft of everyday consumer items" (Finklea 2012) and groups of thieves. The typical ORC organization involves a street team comprised of a thief (the booster), the lookout (the spotter), and a "distractor" whose job it is to draw attention away from booster. Once the goods are removed from the store, the team sells them to Level I fence, who hired the team to take the product. The goods are then sold to a Level II fence, who repackages the goods and transfers them to a Level III fence, who resells them to an unsuspecting public. Not all ORC teams are this elaborate, as one may involve just a booster and a fence. This is a serious crime that costs retailers (and ultimately consumers) tens of billions of dollars each year (The Loss Prevention Foundation 2018). ORC teams typically look for expensive, portable goods in high demand as they are more profitable to steal and more moved and resold.

To combat this, Congress passed the Organized Retail Crime Act of 2008, which made ORC a federal offense, presumed to be a deterrent (Congress.gov 2008). The risks to stores are severe as sales are lost, brands are at risk (name products illegally resold may be damaged, compromised, not warranted, or in poor condition) or contaminated as in the cases of analgesics, baby food, and supplements (The Loss Prevention Foundation 2018).

Retailers provide specific training for this risk for loss prevention teams, store detectives, UCs, security guards, and store staff, so that ORC teams can be detected, deterred, or apprehended.

Audits and Investigations

Security guards and loss prevention specialist conduct audits and investigations, depending in the retail chain, the security contract, and the post orders (Purpura 2002). Investigations may be done on a scheduled or random basis. Audits are typically scheduled and are usually for inventory purposes. For example, a large shipment may be delivered to a store or distribution center and security may conduct an audit to ensure the count of the goods is correct.

Chain of Supply

Security personnel are also responsible for protecting many parts in the retail chain of supply including manufacturing facilities, warehouses,

distribution center, and transportation nodes (trains, depots, airports, trucking, etc.). Security controls access for both staff and vehicles, conduct inventories, do patrols, do safety checks, and conduct drills and evacuations at these facilities. However, technology and growing customer demands have changed this as the "supply chain is not just about distribution and transportation. . .. today's retailers have extensive networks that enable companies to monitor and ensure quality" from retailer to customer (Bandaranayake 2019). This puts additional pressure on security to ensure the safety of goods as they move through the chain in a reliable fashion.

Safety

Security officers are also often responsible for safety in a retail environment as part of an overall risk management program, as "safety is a major loss prevention measure to reduce the likelihood of accidents and injuries" (Purpura 2002). Such a program usually covers risk conditions such as accidents, fire safety, evacuations, active shooter, bomb incidents, workplace violence, safety incidents such as accidents and medical incidents, storms, floods, hurricanes, earthquakes civil disturbances, and power outages. Security personnel are trained to deal with and report such events and to work in coordination with first responders, law enforcement, other businesses in the area, and the community.

Conclusion: The Evolution of Retail Security

The future of retail security looks to combined systems and security personnel with expanded CCTV and alarm systems, robotics, and geo-fencing (electronic attendance systems) for tracking and reporting. Security personnel in retail establishments will be better trained in more sophisticated techniques as technology advances and thieves become more sophisticated in their methods.

Cross-References

- ▶ Investigations: Consumer Retail Shoplifting
- ▶ Retail Security: Employee Theft
- ▶ Retail Security: Shoplifting
- ▶ Security Guards: Authority and Power
- ▶ Security Management

References

American Red Cross. (n.d.). CPR Training. https://www.redcross.org/take-a-class/cpr

Bandaranayake, N. (March 26, 2019). *Supply chain management: Innovations and opportunities*. NRF Foundation. Https://Nrffoundation.Org/Blog/Supply-Chain-Management-Innovations-And-Opportunities

Bhasin, H. (February 6, 2018). 10 types of retail stores. Marketing91. https://www.marketing91.com/10-types-of-retail-stores/

Congress.gov. (2008). H.R.6491 – Organized Retail Crime Act of 2008. https://www.congress.gov/bill/110th-congress/house-bill/6491?s=1&r=21

Dempsey, J. S. (2010). *Introduction to private security*. Belmont: Wadsworth Cengage Learning.

Digital 360 Commerce. (2020). Comparing growth: U.S. ecommerce vs. total retail sales Year-over-year growth, 2010–2019. https://www.digitalcommerce360.com/article/us-ecommerce-sales/#:~:text=Total%20retail%20sales%20increased%203.8,through%20all%20channels%20jumped%204.1%25

EBR-Group.net. (n.d.). *White paper, introduction to exception-based reporting*. Innovative Retail Technologies. https://www.retailitinsights.com/doc/exception-based-loss-prevention-0004

Finklea, K. M. (2012). *Organized retail crime*. Congressional Research Service. https://fas.org/sgp/crs/misc/R41118.pdf

Garcia, T. (February 12, 2019). *U.S retailers lost $300 billion in revenue from markdowns in 2018*. Market Watch. https://www.marketwatch.com/story/us-retailers-lost-300-billion-in-revenue-from-markdowns-in-2018-2019-02-12

Hollinger, R. (October 9, 2018). Sweethearting: The dark side of good customer service. *LP Magazine*. https://losspreventionmedia.com/sweethearting-the-dark-side-of-good-customer-service/

Humphreys, D. (2019). *3 key ways you can use physical security to mitigate the threat of organized retail theft*. Security Today. https://securitytoday.com/articles/2019/02/28/3-key-ways-you-can-use-physical-security-to-mitigate-the-threat-of-organised-retail-theft.aspx?m=1

Kagan, J. (June 14, 2020). Additional insured definition. Investopedia. https://www.investopedia.com/terms/a/additional-insured.asp

Kenton, W. (July 10, 2019). What is inventory? https://www.investopedia.com/terms/i/inventory.asp

Kitteringham, G. (2020). Guard training programs, a development guide. *Security Management magazine*. https://www.asisonline.org/security-management-magazine/articles/2020/07/guard-training-programs-a-development-guide/

LP Magazine. (2020). What is loss prevention. https://losspreventionmedia.com/free-reports/what-is-loss-prevention-retail-loss-prevention-secrets-from-the-experts/

Mazareanu, E. (August 28, 2019). *Security services industry in the U.S. – Statistics & Facts*. Statista. https://www.statista.com/topics/2188/security-services-industry-in-the-us/

McCue, T. J. (January 31, 2019). Inventory Shrink Cost the US Retail Industry $46.8 Billion. Forbes.com. https://www.forbes.com/sites/tjmccue/2019/01/31/inventory-shrink-cost-the-us-retail-industry-46-8-billion/

National Retail Federation. (2020). National Retail Security Survey 2019. https://nrf.com/research/national-retail-security-survey-2019

Penizotto, C. (June, 2020). The Robin Hood Dilemma of Retail. *Loss Prevention Magazine*. https://losspreventionmedia.com/the-robin-hood-dilemma-of-retail/?utm_source=ActiveCampaign&utm_medium=email&utm_content=The+Robin+Hood+Dilemma+of+Retail&utm_campaign=LPM+Daily+2006224

Progressive Grocer. (May 22, 2006). Cashier error leading cause of "bottom of the basket" shrink: PG Webinar Poll. https://progressivegrocer.com/cashier-error-leading-cause-bottom-basket-shrink-pg-webinar-poll

Purpura, P. P. (2002). *Security and loss prevention*. Woburn: Butterworth-Heinemann/Elsevier.

Resume Resource. (n.d.). Retail cashier job description. https://www.resume-resource.com/retail-cashier-job-description/

Secure Community Network. (n.d.). Vetting personnel & vendors. https://securecommunitynetwork.org/resources/best-practice-archive/vetting-personnel-vendors

SecurityGuard-License.org. (n.d.). Security guard license requirements. https://securityguard-license.org/

Seivold, G. (June 10, 2019). Post orders that don't reflect real world activities are a legal ticking time bomb. https://losspreventionmedia.com/post-orders-that-dont-reflect-real-world-activities-are-a-legal-ticking-time-bomb/

Sennewald, C. (2003). *Effective security management*. Burlington: Butterworth-Heineman.

Sennewald, C. A., & Christman, J. H. (2008). *Retail crime, security, and loss prevention: An encyclopedic reference*. Burlington: Butterworth-Heineman.

Spadanuta, L. (July, 2010). Is observe and report good policy? Security Management. https://assisonline.org/security-management-magazine/articles/2010/07/is-observe-and-report-good-policy/

The Loss Prevention Foundation. (July 16, 2018). What is organized retail crime? https://losspreventionmedia.com/lp-101-organized-retail-crime/

Young, J. (February 19, 2020). US Commence Sales Grow 14.9% in 2019. Digital 360 Commerce. https://www.digitalcommerce360.com/article/us-ecommerce-sales/#:~:text=Total%20retail%20sales%20increased%203.8,through%20all%20channels%20jumped%204.1%25

Risk Analysis: National and International Standards

Lusiella Fazzino[1] and Bernard A. Jones[2]
[1]St. John's University, Jamaica, NY, USA
[2]Division of Criminal Justice, Legal Studies and Homeland Security, College of Professional Studies, St. John's University, Jamaica, NY, USA

Keywords

Risk · Risk evaluation · Risk treatment · Risk analysis · Risk management · International Organization of Standards · ISO · ISO 31000:2009 · ISO 31000: 2017e · ISO 31000:2018 · American National Standards Institute · ANSI

Definition

Risk and risk analysis: According to the International Organization for Standardization (ISO 31000: 2009), risk is "the effect of uncertainty on objectives," and risk analysis is "the process to comprehend the nature of risk and to determine the level of risk." Simply put, risk analysis involves understanding the possibilities of risk and the ability to measure their level in relation to an organization's objectives.

Introduction

In this ever-changing and complex world, the threat landscape continues to evolve. With the myriad of natural and human-made threats, organizations must be aware of the threat landscape and the frequency and impacts these threats present. Additionally, the concept of risk is also essential to consider and address as each threat

presents a measure of risk. As stated in the definition above, it is the analysis of risk which allows organizations the ability to meet organizational objectives. In summary, organizations, both large and small, have business objectives to achieve, and to help fulfill those objectives, it is vital to understand the threat landscape and, therefore, proactively conduct a risk analysis.

Completing a risk analysis to assess an organization's current level of risk maturity can no longer be viewed as a trivial or cursory initiative. With more robust financial, operational, and regulatory requirements present, organizations are mandated to conduct comprehensive risks analysis efforts and, in some cases, implement a risk management process and program, which continually monitor, assess, and report on risks to the organization. When first starting a formal risk analysis process and program, an organization can leverage a framework that includes a well-defined set of standards to follow. Assisting in this endeavor, national and international standards for risk analysis, encompassed within risk management, help organizations of all sizes within all industries.

The objective of this entry is to introduce and articulate national and international standards regarding risk analysis. With this introduction to national and international standards, organizations will learn the component which defines risk analysis as well as the underlying principles, framework, and process.

Risk analysis, risk assessment, and risk management are used interchangeably within the industry, yet within the standards, risk analysis is one aspect of risk management. In 1970, the International Organization for Standardization (ISO) began publishing international standards so that they could be adopted nationally (Epstein and Timmermans 2010). ISO is an independent, nongovernmental international organization that creates international standards developed by experts from its 164 countries or member nations (ISO 2015). The standards are intended to be a solution for potential challenges which governments, private industry, and the public may face (ISO 2015). ISO is the "largest international developer and publisher of international standards" and is coordinated by a Central Secretariat based in Geneva, Switzerland (Gjerdrum 2018).

Global-centric, there are 120 member bodies, 40 correspondent members, and 4 subscriber members of ISO. Each nation has one member, and the full member bodies "influence ISO standards development and strategy by participating and voting in ISO technical and policy meetings" (ISO n.d.). A trusted source, ISO has published more than 21,000 standards (Graz and Hauert 2019).

According to ISO, standards are reviewed every 5 years. They are edited by technical experts who are nominated by ISO's members. These experts form technical committees that are responsible for a specific area of expertise (ISO 2015).

It is important to note that ISO is considered the authoritative institute for standards and that many countries adopt or model the ISO standard as their national standard.

In addition to 31000: 2018 Risk Management, ISO/ TC 262 has developed "ISO/TR 310004: 2013 Risk Management – Guidance for the Implementation of ISO 31000" and "IEC 31010: 2009, Risk management – Risk assessment techniques" (ISO n.d.). ISO 31000 Risk Management is, intentionally, a broad standard, as opposed to specific, in order to ensure that "the needs of any type of organization or situation" are met (Lalonde and Boiral 2012).

In order to remain current and advance standards like risk management, there are many meetings, drafts, and inputs given to reach consensus, over a 3-year period typically (Esposito 2017). The standards are reviewed and published again every 5 years (Esposito 2017). This rigorous evaluation and updating from industry experts and member nations keeps the standards current and in line with the most recent developments in all aspects of risk management and risk analysis.

The American National Standards Institute (ANSI) is a national organization. It adopts international ISO standards and authorizes US participation in the standards-making process (Gjerdrum 2018). Technical Advisory Groups (TAG) are also formed within ISO. The American Society of Safety Professionals (ASSP), a US leader in the development of risk management and risk analysis best practices, is the secretary to this TAG

group of experts, in the United States, who participate in the ISO 31000 standards-making process (Gjerdrum 2018). At the national and international levels, governmental, academic, and industry interests are broadly represented.

ANSI provides a significant benefit to organizations with the standardization of new and emerging technologies. As new standards are introduced, organizations as well as government agencies can create products and services to meet or exceed the ANSI standards. For example, the standardization services that ANSI provides help to ensure that computer manufacturers build components which will be compatible with other third-party components. The process by which a new standard is accredited by ANSI is a rigorous one and helps to ensure that both consumers and manufacturers are presented with a standard that has passed stringent guidelines. This is important as industry standards help ensure a level of uniformity across technology which provides a measure of risk mitigation.

National Standards Related to Risk Management

In 2011, the ISO 31000 standard was published as ANSI 690.2 in the United States (Esposito 2017). Recognizing the precision and completeness of the international standard, the United States adapted it without any modification. The national ANSI 690.2 standard's approach to the risk management principles, framework, and process follows the approach put forth by ISO 31000:2009.

International Standards Related to Risk Management

ISO 31000

An organization protects and creates value by successfully managing risk (Gjerdrum 2018). In pursuit of an organization's goals and objectives, it is paramount to have a shared understanding of risk management (Gjerdrum 2018). This includes the ability to identify risks across all operations; knowing when it is appropriate to undertake risk; knowing who is in the best position to manage specific risks; and knowing which people are accountable for risk (Gjerdrum 2018). All organizations face factors and influences that jeopardize whether it will achieve its objectives – some risks are external and some are internal (Gjerdrum 2018). Risk management supports the achievement and organizational objectives by understanding those uncertainties and managing their effects upon the organization and its operations (Gjerdrum 2018). Organizations manage risk in order to protect or preserve value: maintain public trust; protect people and assets; and to focus on the cost of risk (Gjerdrum 2018).

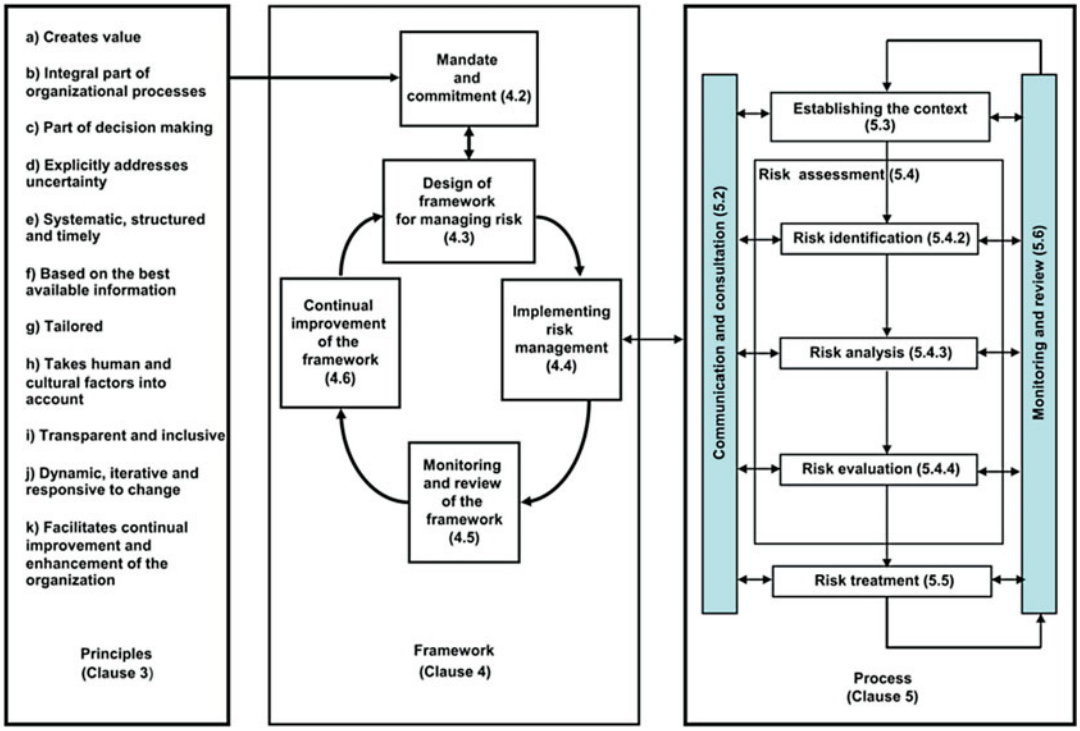
ISO 31000 is a general standard, intended to address all types of challenges, including "threats to the environment, public health and food safety issues, threats to critical infrastructure, hazards presented by certain products, and interruption of the supply chain" (Lalonde and Boiral 2012). This standard can be used by any industry, sector, or profession: security, IT or fire risk assessment; corporate, military, emergency, storms, business interruptions, oil wells, police, and even personal risk (Esposito 2017).

ISO 31000 encourages consideration of what you may already have in place for risk management and how to more fully coordinate and integrate that effort. The focus in ISO 31000 is to manage risk in relation to the mission and objectives of an organization. Risk management supports taking risks and good decision-making. In the United States, the term "Enterprise Risk Management" (ERM) is used, and although it is different than the international verbiage, they are, in practice, the same thing (Gjerdrum 2018).

ISO 31000:2009

Based on a standard which Australia and New Zealand developed called AS/NZS 4360, the ISO 31000: 2009 Risk Management Standard is an international guideline. Over 60 countries have adopted it as their national risk management standard (Hutchings 2016).

There are three distinct parts which form the standard for risk management: the Principles, Framework, and Process as seen in Fig. 1 as Clause 3, Clause 4, and Clause 5. Further, the


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
Framework (Clause 4)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
Process (Clause 5)

Risk Analysis: National and International Standards, Fig. 1 ISO 31000: 2009 Risk Management-principles (ISO 2009)

ISO 31000 Risk Management Standard is used as a reference for many ISO families of standards (Hutchings 2016).

Principles

The risk management principles (Clause 3, Fig. 1) of ISO 31000 provide the "foundation of the work and describe the qualities of effective risk management" (Gjerdrum 2018). According to Esposito (2017), this is "why" we engage with risk management. As seen in the first box to the left in Fig. 1, ISO 31000: 2009 revolves around 11 principles of risk management that can be customized. By design, these principles remain flexible so they can fit any organizational context. A plan for risk management does the following (ISO 2009):

(a) Creates value
(b) [Is an] Integral part of organizational processes
(c) [Plays] part in decision-making
(d) Explicitly addresses uncertainty
(e) [Is] systematic, structured, and timely
(f) [Is] based on the best available information
(g) [Is] tailored
(h) Takes human and cultural factors into account
(i) [Is] transparent and inclusive
(j) [Is] dynamic, iterative, and responsive to changes
(k) Facilitates continual improvement and enhancement of the organization

These principles serve as a guideline or foundation for an effective risk management framework and process, which may be used with any service or product (Hutchings 2016).

Framework

The risk management principles (listed above a–k) are then translated into a risk management "framework" as seen in the middle box (Clause 4) of Fig. 1 (Esposito 2017). What is included in one's organizational written plan regarding risk management would address each of the five smaller boxes in the framework: "4.2 Mandate and

commitment, 4.3 Design of framework for managing risk, 4.4 Implementing risk management, 4.5 Monitoring and review of the framework and 4.6 Continual improvement of the framework" (ISO 2009). The risk management framework exemplifies "what" needs to be done to effectively engage in risk management. The following is a brief explanation of each component of the "framework."

4.2 Mandate and Commitment. The possibility that risk management may be mandated by a regulatory or governmental body needs to be considered. If there is leadership commitment within an organization, that commitment must be defined.

4.3 Design of Framework for Managing Risk. Outlining the organizational framework is crucial. This includes identifying who will be assessing and maintaining any suggested action plans, sharing relevant data, and deciding how often that data will be made public (Esposito 2017).

4.4 Implementing Risk Management. Determining the persons who possess the skill set needed to implement the risk management is paramount (Esposito 2017).

4.5 Monitoring and Review of the Framework. Ongoing monitoring and review of the framework must occur, and, if necessary, inspections and review of the steps involved are made (Esposito 2017).

4.6 Continual Improvement of the Framework. Finally, implementing an audit process to review and improve the risk management process every couple of years is recommended as a best practice (Esposito 2017).

The risk management framework provides for "consistent integration across the organization" and is likened to a "big picture integration" (Gjerdrum 2018). It is iterative in nature and fluid, as demonstrated by the arrows in the clockwise sequence.

Process

According to Esposito (2017), the risk management process (Clause 5), in the right box of Fig. 1, is "how" you engage in risk management. It can be viewed as the "steps taken to "evaluate and review risks," whether they are individual or in a portfolio (Gjerdrum 2018). As described in the previous section, the principles of risk management influence how an organization implements the risk management process (Gjerdrum 2018). The risk management process includes the following, which will be explored: "5.2 Communication and Consultation; 5.3 Establishing the Context; 5.4 Risk Assessment (including 5.4.2 Risk Identification, 5.4.3 Risk Analysis, and 5.4.4 Risk Evaluation); 5.5 Risk Treatment; and 5.6 Monitoring and Review" (ISO 2009).

5.2 Communication and Consultation. A key component for stakeholder "buy-in" is their involvement in the development of a treatment plan. Communication and consultation with all interested parties is essential: stakeholders, employees, and management (Esposito 2017).

5.3 Establishing the Context. Definitions for each item in this box must be set, and ascertaining how the organization will meet its objectives is key (Esposito 2017). Identification of the external and internal parameters that are considered when looking at risk management is also vital (Esposito 2017). This can be regulatory or legislative, for example.

5.4 Risk Assessment. Risk assessment occurs when there is 5.4.1 Risk Identification, 5.4.2 Risk Analysis, and 5.4.3 Risk Evaluation.

5.4.1 Risk Identification The risk identification process which the organization or situation utilizes must be determined (Esposito 2017). A survey of how an organization analyzes risk to identify the hazards and hazardous situations or events is needed (Esposito 2017). Some examples of methods used for risk identification are brainstorming; look-up methods like checklists or hazard analysis which are common in the United States; scenario analysis like "what if"; and controls' methods where the control is studied to see if risk is truly mitigated by its use (Esposito 2017).

5.4.2 Risk Analysis Risk analysis informs the decision of which risks are worth pursuing and which should be avoided (Sadgrove 2016). Some other factors that need consideration are the matrix that will be used, the definition of likelihood, and the potential consequences (Esposito 2017).

Risk is then evaluated to determine whether enough is being done to manage the risk (Gjerdrum 2018). If not, then you consider the next box (Clause 5 in Fig. 1), risk treatment. In risk treatment, some risks may be worth supporting, and in other situations, there may be considerations of how to minimize the threat (Gjerdrum 2018). This is discussed in further detail in the Best Practices section (see Fig. 6).

5.4.3 Risk Evaluation The ability to determine what level of risk is acceptable or tolerable is called risk evaluation. Controls are selected to test risk level and help decide if additional treatment may be necessary. This is one step that is often overlooked, but it is a best practice, often taking place as compliance or an industry practice (Esposito 2017). You may have reduced the likelihood of a risk, but you have not reduced its potential severity unless there is an evaluation of controls (Esposito 2017).

According to Esposito (2017), the most preferred and reliable controls to the least are as follows:

(a) "Risk avoidance
(b) Elimination
(c) Substitution
(d) Engineering controls/safety devices
(e) Warning
(f) Administrative controls (e.g., in work, supervision, training)
(g) Personal protective equipment (PPE)"

Most people do their first risk assessment by utilizing these controls. The risk is identified, analyzed, and evaluated (Esposito 2017).

5.5 Risk Treatment. Once a risk is identified, management then decides how much funding will be allocated toward treating that risk (Esposito 2017). A treatment plan may include documenting proposed actions; assigning responsibilities, resources, and performance measures; reporting and monitoring; and timing (Esposito 2017).

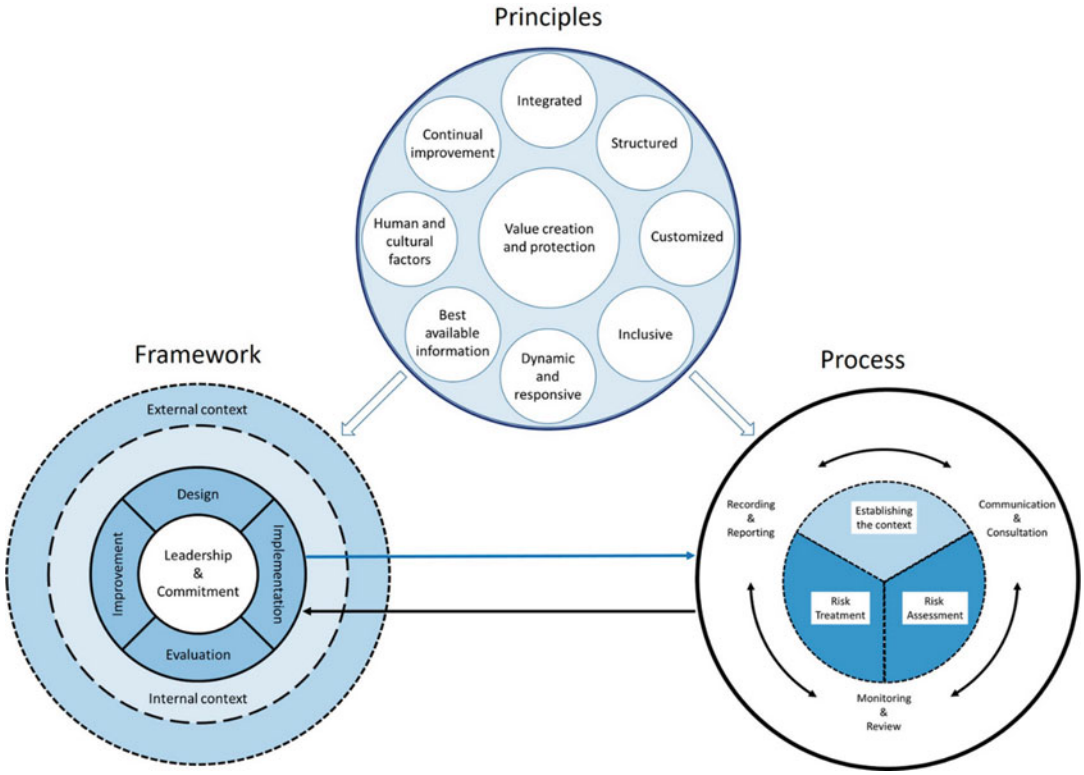
5.6 Monitoring and Review. The person or department that will monitor and review, as well as the person who shares any data or updates, must be established (Esposito 2017). Before ISO 31000: 2009, traditional risk management administration was perceived as a "department of no" (Gjerdrum 2018). The focus of risk management was on preventing and transferring risk because risk was generally perceived as bad (Gjerdrum 2018). With ISO 31000, however, risk owners are engaged to manage risks and risk is perceived as either good **or** bad (Gjerdrum 2018). Risk-taking and good decision-making are supported by the ISO 31000 Risk Management Standards, and the focus is on risk in relation to the organizational mission and objectives (Gjerdrum 2018).

Risk Management: Changes in Policy and Procedures

ISO 31000:2017 (e), Draft of ISO 31000:2018

Five years after the ISO 31000: 2009 publication, work began on its revision in 2014 by the ISO Technical Committee (TC) 262 (Gjerdrum 2018). There was a move away from jargon so that its language and concepts would be more accessible to all readers and organizations (Gjerdrum 2018). Of note were the past linguistic, cultural, and local differences and interpretations of the ISO language used which conflated the standard's meaning. The images used to illustrate ISO 31000 went through one iteration in the draft, 2017(e), (Fig. 2) and then was finalized in 2018 (Fig. 6).

The most noticeable change was using a circular model rather than square. For each of the ISO 31000 components (principles, framework, and process), a core was created that is central in each distinct component. The iterative and holistic nature throughout all the risk management concepts is emphasized with the use of arrows: moving from the Principles to inform



Risk Analysis: National and International Standards, Fig. 2 ISO/DIS 31000:2017 Risk Management-guidelines Draft (ISO 2017)

both the Framework and Process; arrows pointing back and forth between the Framework and Process; and arrows moving in clockwise and counterclockwise directions within the Process component.

Principles

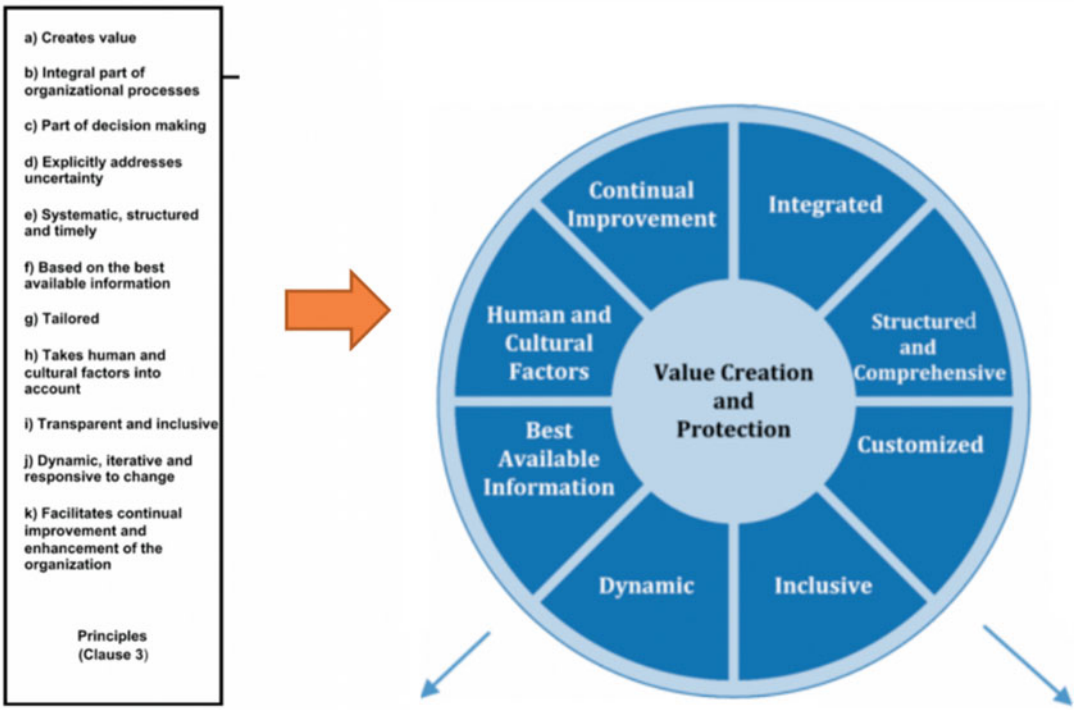
Risk management has traditionally referred to protection where risk was viewed as negative and the goal was to transfer away from risk (Gjerdrum 2018). Changing from (Clause 3) Principles in Fig. 1, the new ISO 31000: 2017(e), Fig. 2, and eventual ISO 2018, Fig. 3, includes value creation at its core, together with protection (Gjerdrum 2018). Risk is seen as uncertainty, and it can be optimized to reach organizational objectives (Gjerdrum 2018). There is an emphasis on objectives; prioritizing activities and budgets; support in taking risks and making better decisions; and driving innovation and leadership (Gjerdrum 2018).

Value creation and protection are at the core of the image and refer to the assets and objectives of the organization (Esposito 2017). Esposito (2017) explains that less downturns and negative events are the goal of value creation and protection.

Overall definitions in the Principles section were reduced from 29 to 8. Definitions which were commonly understood and seemed duplicative were removed (Gjerdrum 2018). Other terms were simplified, such as tailored being replaced with customized, for greater clarity and less confusion (Gjerdrum 2018). In summary, although the language was made clearer and more concise, the chronological and linear nature of Risk Management Principles was replaced by a looser and more iterative model.

Framework

At the core or nucleus of the Risk Management Framework component are leadership and


a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Continual Improvement
Integrated
Structured and Comprehensive
Customized
Inclusive
Dynamic
Best Available Information
Human and Cultural Factors
Value Creation and Protection

Risk Analysis: National and International Standards, Fig. 3 Comparison between Principles 31000:2009 (ISO 2009) and ISO 31000: 2018 (ISO 2018)

commitment. If management is not committed to risk management, then it will not be effective.

Previously, in ISO 31000: 2009, there was only input from the Principles into the Framework, and now, with ISO 31000: 2017 (e), Fig. 2, and ISO 2018, Fig. 4, all aspects of the Risk Management Process can also be incorporated into the Framework and all aspects of the Framework can be incorporated into the Process. They are all interrelated.

"Mandate and Commitment" is now "Leadership and Commitment" because not every organization will issue a "mandate" for risk management (Gjerdrum 2018). The term mandate implies policy, whereas leadership is more realistic and flexible, making it customizable (Gjerdrum 2018). "Monitor and Review" are now "Evaluation" as there was a concerted effort to use terms tied to business objectives: Design, Implementation, Evaluation, and Improvement (Gjerdrum 2018).

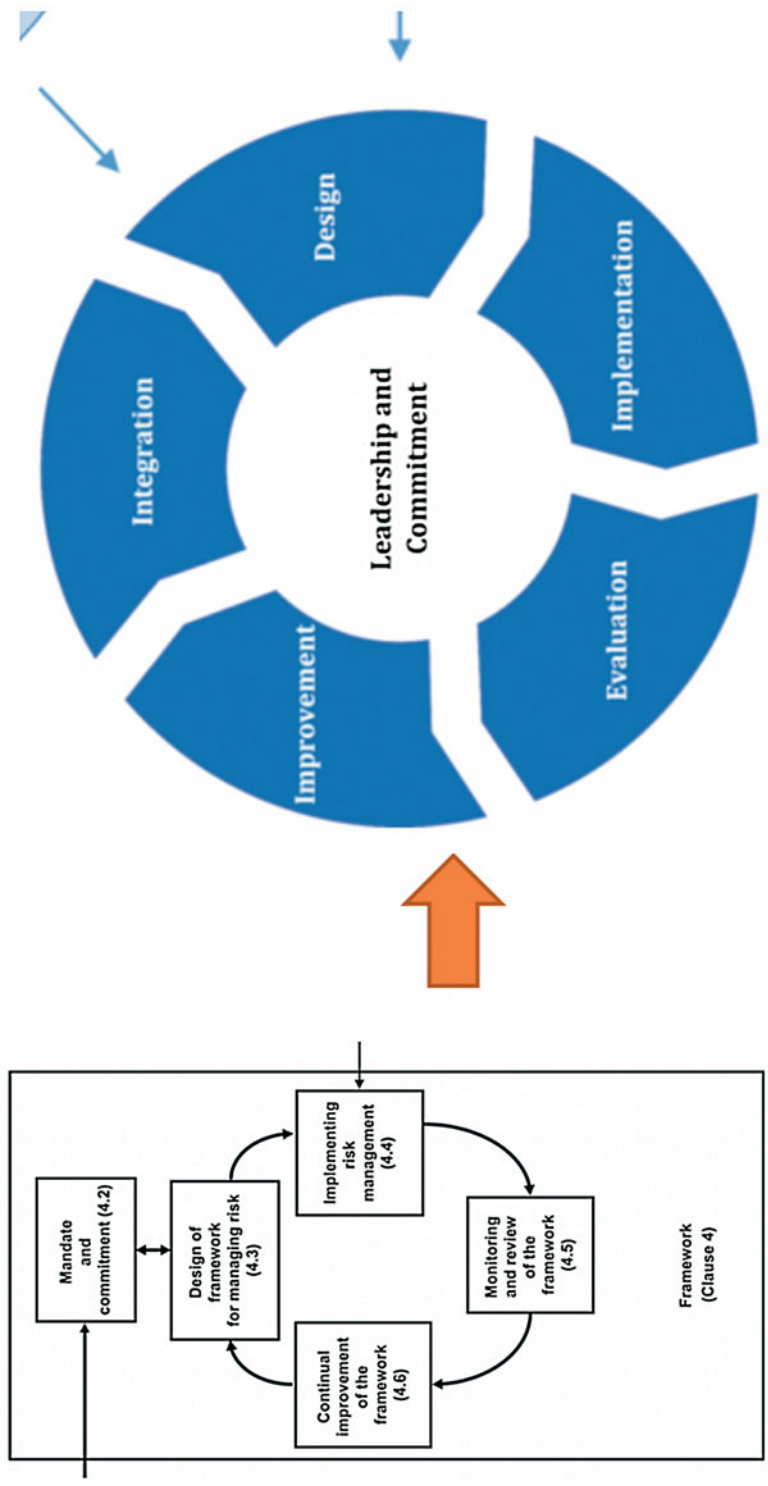
Risk Management Process

Risk may be managed well at your organization, but there may be some steps which are overlooked. The risk management process can be improved by going through the process steps according to ISO 31000. The scope, purpose, context, and criteria, in the top small light blue box of Fig. 5, need to be set before work begins on the risk management process to identify and analyze risk (Gjerdrum 2018). Everyone in the organization benefits from understanding which uncertainties are potentially most critical and may need attention. The management of risk should be incorporated at every level of the organization – from broad a strategy setting to individual decision-making.

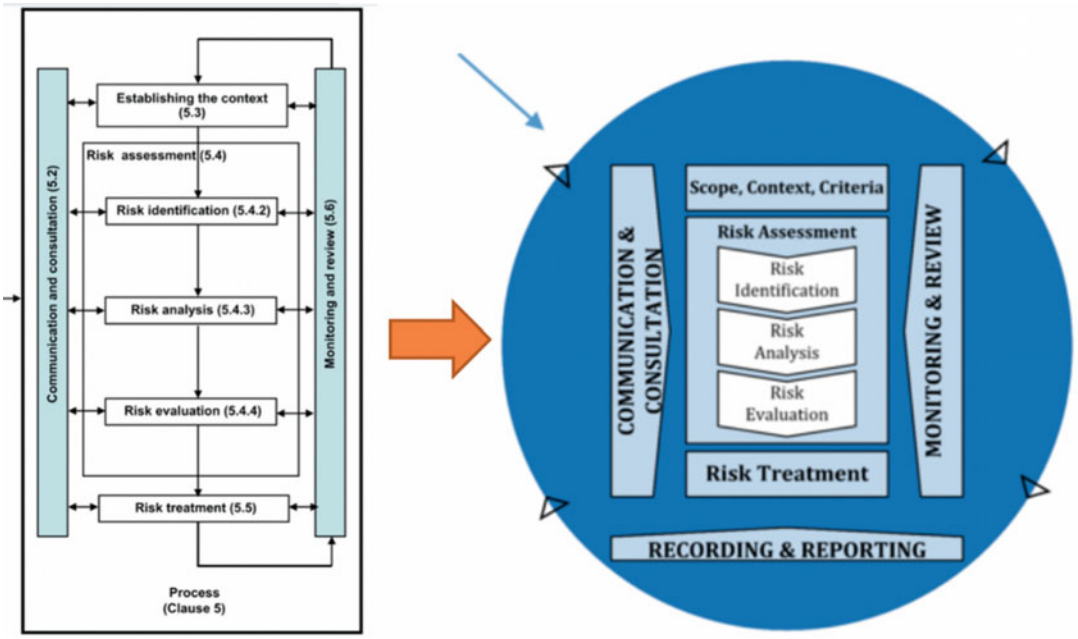
Best Practices Overview

ISO 31000:2018

Between ISO 31000: 2017 (e) and ISO 31000: 2018, minimal changes were made, and the new Risk Management Standard was to be integrated into all organizational activities, especially decision-making (Gjerdrum 2018).



Risk Analysis: National and International Standards, Fig. 4 Comparison between Framework 31000:2009 (ISO 2009) and ISO 31000:2018 (ISO 2018)



Risk Analysis: National and International Standards, Fig. 5 Comparison between Risk Management Process 31000:2009 (ISO 2009) and ISO 31000:2018 (ISO 2018)

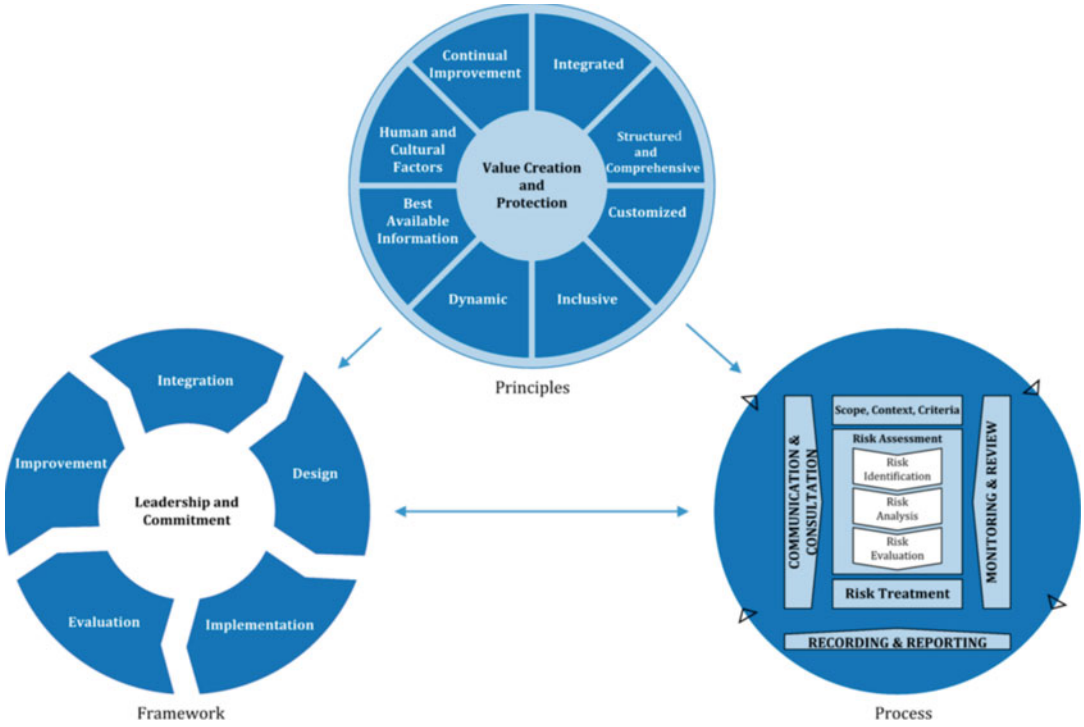
The chair of the technical committee on risk management (ISO/TC 262), Jason Brown, states that the revised version of ISO 31000, Fig. 6, focuses on integration within the organization in relation to the role of leaders and their responsibilities. Its "open system" approach lets it be effectively applied on multiple levels and in several national contexts (Brown 2017). Risk management has become an integral part of business (Stanchard 2018).

The 2018 version is much shorter than the previous 2009 standard, and there were many improvements in preciseness and language (Brühwiler 2017). The generic and "user-friendly" qualities of ISO 31000: 2018 exemplify its evolution. The principles also "inform both the framework and process" of ISO 31000, influencing "the structure and design of the framework for managing risk" (Gjerdrum 2018).

The Risk Management Framework was updated to emphasize integration throughout the organization (Gjerdrum 2018). The model used includes aspects of leadership and management that are more central to risk management (Gjerdrum 2018). Understanding the scope and the context and setting risk criteria *before* working through the risk management process is crucial (Gjerdrum 2018). Recording and reporting were also added and made more explicit (Gjerdrum 2018).

Designing an ISO 31000 Risk Management Framework calls for risk knowledge, skills, and abilities that must be customized to an organization's unique context (Hutchings 2016). Gjerdrum (2018) states that many times, the Framework is established before implementing a policy of how it is going to happen because most organizations are not policy driven nor do they have mandate or compliance concerns.

A new focus with 2018 is the shift to consider stakeholder views, perceptions, and interests as part of a risk management framework, program, and process (Gjerdrum 2018). Stakeholders are people and organizations "that can affect, be affected by, or perceive themselves to be affected by a decision or activity" (Gjerdrum 2018). Stakeholders can be internal (employees) and external (government and regulators) and need to be



Risk Analysis: National and International Standards, Fig. 6 ISO 31000:2018 (ISO 2018)

accounted for in any risk management process (Gjerdrum 2018).

The risk management process focuses on risk assessment (Gjerdrum 2018). In the risk assessment portion of the risk management process, risks are identified and defined. There is an analysis of whether those risks will happen and, if so, how serious they might be (Gjerdrum 2018). When doing risk analysis, risk is put into distinctive buckets, as illustrated in Table 1 (Esposito 2017).

Here, tolerance of risk is measured. If there is high risk, the activity is not permissible, the job must be stopped, or there may be continuous oversight and monitoring (Esposito 2017). If there is a serious or medium risk, the risk may be allowable, but one should be continuously looking for ways to improve or reduce the risk (Esposito 2017). Controls such as elimination, substitution, and barriers must be looked at, and multiple layers of protection may be implemented (Esposito 2017). If there is a low risk, the organization may choose to have exposure and use

Risk Analysis: National and International Standards, Table 1 Risk analysis – consequence/probability matrix (Esposito 2017)

Risk	Definition	Example
High	Operation not permissible	Stop the job. Continuous oversight. Defense in depth or layers of protection
Serious	High-priority remedial action	Controls such as elimination, isolation, substitution, and barriers are preferable. Defense in depth or layers of protection
Medium	Take remedial action at appropriate time	Utilize hierarchy of controls. If controls are limited to administrative or personal protective equipment (PPE), add defense in depth or layers of protection
Low	Risk acceptable, remedial action discretionary	May be able to rely on administrative and PPE controls

controls such as administrative influence or personal protective equipment (PPE) (Esposito 2017).

Ultimately, with ISO 2018, a more permeable and accessible standard for risk management has been formed which takes into account the unique characteristics of a setting or organization regardless of where it is situated in the world.

Conclusion

Today's landscape of both natural and human-made threats continually presents levels of risk to organizations. With threats becoming more complex, organizations must understand the importance of risk analysis to help address those threats. There is little doubt that organizations that do not adapt risk analysis processes and planning will be ill-equipped to address future threats and minimize disruption to operations. As articulated within this entry, comprehensive and sound risk analysis is built upon national and international standards. These standards provide guidelines ensuring that risk managers have a vetted and comprehensive framework to leverage in which conducting organizational risk analysis initiatives.

Differences in policy and procedure among national and international standards are a result of the competing, varying needs and interests of stakeholders and locales. Stakeholders may include legislative bodies, insurance companies, consumers, shareholders, management, employees, trade unions, nongovernmental organizations, industry, the public, and much more. While participation on TC 262, the technical committee which oversees ISO 31000, is "formally open to all interested parties, voluntary market actors and expert knowledge largely dominate standardization committees" (Hauert et al. 2013).

Organizations use standards to "ease transactions and to structure their internal affairs as well as the world around them" (Botzem and Dobusch 2012). However, "reconciling the international scope of standards devised within ISO with strategies geared to national or regional projects and regulations is a challenge" (Graz and Hauert 2019). There is "great diversity once you get below the principles and framework" [of ISO 31000] and the "quality of application is affected by experience and local conditions" (Brown 2017). Plainly, international standards like ISO 31000, while intended to be both macroscopic and microscopic in nature, can sometimes fall short in local and granular instances.

One of the challenges of risk management is that various sectors have very disparate understandings of risk management and even speak in dissimilar ways about it (Marinelli 2017). Most areas see risk only "from the negative standpoint and are repelled by the standard as soon as they read the risk definition" (Marinelli 2017). Managers are sometimes "unaware or are not ready to recognize risks" because risk is contrary to their ambitions and strategic goals (Brühwiler 2017). Risk perception is challenging because outcomes and deliverables are generally focused on positive results. Risk is rarely seen as positive or as opportunity to grow.

Adding practical examples of implementation of a standard may remedy any vagueness which may be perceived. Explaining positive risk and explaining how it allows for opportunities is the "only way people outside the risk management will be able to embrace the standard" (Marinelli 2017). While stakeholders may include everyone affected by the standards, ISO 31000 has come from an area of industry which can also be viewed as problematic because local elements can be overlooked in standardization (Marinelli 2017). From financial and insurance industries to government to public and private organization to universities, to urban planning sectors, ISO 31000 is viewed as accommodating and not obstructive. The ISO 31000 Standard brings more harmony than discord to the global order of risk management. The evolution and flexibility of the Standard allows it to be adapted in an array of situations, organizations, and geographic settings.

Cross-References

- ▶ Emergency Management: Best Practices
- ▶ Fraud Risk Management: Using Fraud Analytics to Combat External and Insider Threats

- ▶ Influence of Risk Perception on Event Risk Management and Decision-Making
- ▶ Maritime Security: Acceptable Risks

References

Botzem, S., & Dobusch, L. (2012). Standardization cycles: A process perspective on the formation and diffusion of transnational standards. *Organization Studies, 33*(5–6), 737–762.

Brown, J. (2017). Risk management and TC 262 [Interview]. Retrieved from https://committee.iso.org/files/live/sites/tc262/files/Documents/Interview%203.pdf

Brühwiler, B. (2017). The ongoing revision of ISO 31000 [Interview]. Retrieved from https://committee.iso.org/files/live/sites/tc262/files/Documents/interview%201.pdf

Epstein, S., & Timmermans, S. (2010). A world of standards but not a standard world: Toward a sociology of standards and standardization. *Annual Review of Sociology, 36*, 69–89. https://doi.org/10.1146/annurev.soc.012809.102629.

Esposito, P. [ASSP Safety]. (2017, March 21). *ISO 31000 risk management what changes may be on the way* [Video file]. Retrieved from https://vimeo.com/276505906

Gjerdrum, D. [ASSP Safety]. (2018, September 17). *The international stand on risk management, ISO 31000: 2018* [Video file]. Retrieved from https://vimeo.com/290489362

Graz, J.-C., & Hauert, C. (2019). Translating technical diplomacy: The participation of civil society organisations in international standardisation. *Global Society, 33*(2), 163–183. https://doi.org/10.1080/13600826.2019.1567476.

Hauert, C., Audétat, M., Bütschi-Häberlin, D., Graz, J. C., & Kaufmann, A. (2013). Civil society organisations participating in ISO TC 228 and ISO TC 229: The INTERNORM project and its future. In *EURAS proceedings 2013* (pp. 171–186). Aachen: Verlag Mainz.

Hutchings, G. (2016). *ISO 31000: Enterprise risk management*. Portland, OR: Quality Plus Engineering.

International Organization for Standardization (2015). International Organization for Standardization: ISO Strategy 2016-2020 (Brochure). Geneva, Switzerland. ISBN 978-92-67-10638-0.

International Organization for Standardization. (2018). ISO 31000 – Risk management. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO TC STANDARDS by ISO TC 262 Risk Management. (n.d.). Retrieved from https://www.iso.org/committee/629121/x/catalogue/

ISO Technical Management Board Working Group on Risk Management. (2009). ISO 31000:2009(en): Risk management – Principles and guidelines. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

ISO: About Us – Members. (n.d.). Retrieved from https://www.iso.org/members.html

Lalonde, C., & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. *Risk Management, 14*(4), 272–300. https://doi.org/10.1057/rm.2012.9.

Marinelli, V. (2017). Risk management and ISO 31000 in Argentina. [Interview]. Retrieved from https://committee.iso.org/files/live/sites/tc262/files/Documents/interview%208.pdf

Sadgrove, K. (2016). *The complete guide to business risk management*. New York, NY: Routledge.

Further Reading

Fraser, J., & Simkins, B. (2010). *Enterprise risk management today's leading research and best practices for tomorrow's executives*. Hoboken: Wiley.

Hutchins, G. (2018). *ISO 31000:2018 enterprise risk management CERM academy series on enterprise risk management*. Quality + Engineering/CERM Academy. Portland, OR.

Robots

Marie-Helen Maras
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Robots · Critical infrastructure · Privacy · Security

Definition

Robots are machines with computer software that are designed to automatically perform a variety of noncomplex and/or complex tasks.

Introduction

Robots are machines with computer software that are designed to automatically perform a variety of noncomplex and/or complex tasks. Some robots look like machines (e.g., SoftBank Robotics' Pepper and Knightscope's Rosie), while others are anthropomorphic (e.g., Hanson Robotics' Sophia)

(Fouraker 2018; Son 2018). Robots are deployed in public and private sectors around the world to cut costs associated with human labor and to enhance the efficiency of operations. Robots are predominately built to enable their real-time and remote access for efficiency purposes. The real-time and remote access of robots adversely impacts the security of these objects and the privacy of data aggregated, analyzed, and shared by these objects.

Robots in Critical Infrastructure Sectors

Robots have been deployed in many critical infrastructure sectors for a variety of reasons. In the commercial sector, robots are used in certain subsectors, such as retail and lodging. For example, robots have been used in the hospitality industry (e.g., hotels). Japan is famous for its hotels with robots, which not only check-in guests, clean rooms, store luggage, and bring luggage and other items to guests' rooms, but are also located within the guests' rooms to provide them with services (Choi et al. 2020; Malaea 2019). During the 2020 coronavirus pandemic, robots were used in Japan to greet coronavirus patients placed within hotels (Reuters 2020). Some US hotels also use robots to deliver items to guests' rooms, among other activities (Martin 2016). In addition, robots have been used in the: healthcare sector to conduct remote robotic assisted surgeries; manufacturing of goods, such as cars and digital technology; financial sector for customer service (e.g., Pepper has been deployed in HSBC banks branches); transportation sector, particularly the airports to provide travelers with flight and airport information and to clean airports; and defense sector, where robots deliver goods and services, and even medical care in battlefields (Son 2018; Fouraker 2018; Babe 2017; Holmes 2020; D'Monte 2015; Creswell et al. 2018; Beiser 2018; Sykes 2018).

Moreover, robots are used for security and emergency management purposes. For instance, Talon and PackBot robots are used in border security to investigate tunnels found at the US border, which are used to illegally smuggle drugs, weapons, and people into the country (McNeill and Machi 2009). These robots conduct reconnaissance and can relay information about what they find back to the agency that is using them. Furthermore, robots are used in natural and human-made disaster response because they can traverse hazardous terrains and provide relief and/or monitor locations where it is unsafe for humans to be (e.g., locations with extreme radiation levels that would cause harm to human beings).

Security Concerns

Many robots were not built with cybersecurity and/or security in mind. Because of this, robots are susceptible to cybersecurity threats because they can be remotely accessed for maintenance and operation. A case in point are the vulnerabilities identified in the in-room robots of Japan's HIS Group hotel chain. Specifically, the vulnerabilities enabled remote access to the in-room robots and enabled perpetrators to control the camera and microphone in order to see and listen to the guests in the rooms (Parrish 2017). Robots interact with their immediate environments and collect and process contextual information to operate within these environments. These operations result in the vast collection, processing, and ultimately sharing of contextual information. The privacy implications of the collection of these vast quantities of data needs to be considered.

Robots are further vulnerable to supply chain risks, from the design of the product, to its development, to the creation of the final product. One such risk involves vendors that provide critical components for robots (e.g., microcontroller). For instance, outsourcing these components to a company that is located in a foreign country can provide the foreign country with the ability to introduce a hardware vulnerability that could be exploited by the country at a later date. Software or hardware with malware may also be used to create the robots and/or the software applications used with robots may be vulnerable to cyber-attacks. Vulnerabilities in third party applications required for the monitoring and remote

operation of robots may also be present. Interconnections of robots to other digital technologies, and even other robots, create new vulnerabilities. These vulnerabilities include the interception of data being transferred, the surreptitious monitoring of data, and the gaining of unauthorized access to the administrative capabilities of the robots. The vulnerabilities enable perpetrators to surveil the environment within which they operate and/or control the functions of the robots in order to modify, disable, or otherwise interfere with the normal functioning and operations of the robots.

Finally, robots may not operate as intended and/or may malfunction, resulting in damage to property, injury, serious harm, and/or death. There have been several instances of maloperations and malfunctioning of robots. In Alabama, a woman in a factory, Ajin USA plant, was crushed to death by a car-robot, when it restarted as she was trying to determine why it malfunctioned (Silverman 2017). In California, a mall security robot knocked a toddler down and ran him over in the Stanford Shopping Center (McFarland 2016). The toddler sustained minimal injury to the leg. Surgical robots have also malfunctioned causing minor and major injuries, even death (BBC 2015).

Conclusion

The security concerns regarding robots involve both the data processed, stored, communicated, and shared by the robot, and the unauthorized access and use of the robot. Data obtained, processed, and transmitted by the robots should be secured, encrypted, or otherwise obfuscated to protect the confidentiality and integrity of data. Robot security can be implemented at the design level by creating secure firmware and software. Any default usernames and passwords, wherever present, should be changed by the users or operators of the robots. Because unauthorized access to robots can destroy, disrupt, and degrade robot capabilities and operations, robots should be developed in a manner that enables them to withstand cyberattacks.

Cross-References

▶ Cybersecurity: Practice

References

Babe, A. (2017). Why South Korea is an ideal breeding ground for robots. *BBC News*, 6 Dec 2017. http://www.bbc.com/travel/story/20171205-why-south-korea-is-an-ideal-breeding-ground-for-robots

BBC. (2015). Robotic surgery linked to 144 deaths in the US. https://www.bbc.com/news/technology-33609495

Beiser, V. (2018). The robot assault on Fukushima. *Wired*, 26 Apr 2018. https://www.wired.com/story/fukushima-robot-cleanup/

Choi, C., Oh, M., Choi, M., & Kim, S. (2020). Exploring the influence of culture on tourist experiences with robots in service delivery environment. *Current Issues in Tourism*. https://doi.org/10.1080/13683500.2020.1735318.

Creswell, K., Cunningham-Burley, S., & Sheikh, A. (2018). Health care robotics: Qualitative exploration of key challenges and future directions. *Journal of Medical Internet Research, 20*(7), e10410. https://doi.org/10.2196/10410.

D'Monte, L. (2015). 5 Robots that may rescue you from natural disasters. *Government Technology*, 2 June 2015. https://www.govtech.com/em/safety/5-Robots-That-May-Rescue-You-From-Natural-Disasters.html

Fouraker, C. (2018). Robotic security forces on patrol in NYC prompt privacy concerns for some. *CBS New York*, 16 Oct 2018. https://newyork.cbslocal.com/2018/10/16/knightscope-robot-security-patrol/

Holmes, A. (2020). Police robots keep malfunctioning, with mishaps ranging from running over a toddler's foot to ignoring people in distress. *Business Insider*, 19 Jan 2020. https://www.businessinsider.com/police-robots-security-malfunctioning-fails-knightscope-2020-1

Malaea, M. (2019). Quirky Japanese hotel replaces in-room robots when they turn out to be hackable can be turned into peeping toms. *Newsweek*, 23 Oct 2019. https://www.newsweek.com/quirky-japanese-hotel-replaces-room-robots-when-they-turn-out-hackable-can-turned-peeping-toms-1467386

Martin, H. (2016). Cutting edge: Robots deliver fun with hotel room service orders, and they don't expect a tip. *LA Times*, 7 Feb 2016. https://www.latimes.com/business/la-fi-hotel-robots-20160207-story.html

McFarland, M. (2016). 300-Pound mall robot runs over toddler. *CNN*, 14 July 2016. https://money.cnn.com/2016/07/14/technology/robot-stanford-mall/index.html

McNeill, J. B., & Machi, E. (2009). Robotics and the next steps for national security. *Heritage Foundation*. https://www.heritage.org/node/13925/print-display

Parrish, M. (2017). Massive industrial robots vulnerable to being hacked. Manufacturing.net, 3 May 2017. https://www.manufacturing.net/industry40/news/13116550/massive-industrial-robots-vulnerable-to-being-hacked

Reuters. (2020). Robots on hand to greet Japanese coronavirus patients in hotels. https://www.reuters.com/article/us-health-coronavirus-japan-robot-hotels/robots-on-hand-to-greet-japanese-coronavirus-patients-in-hotels-idUSKBN22D4PC

Silverman, G. (2017). A death in Alabama exposes the American factory dream. *The Financial Times*, 5 Feb 2017. https://www.ft.com/content/54d05c3e-e9fa-11e6-893c-082c54a7f539

Son, H. (2018). This bank is staffing branches with humanoid robots that dance, take selfies and push credit cards. *CNBC*, 26 June 2018. https://www.cnbc.com/2018/06/26/this-bank-is-staffing-branches-with-humanoid-robots-that-dance-take-s.html

Sykes, N. (2018). How manufacturing automation is evolving. *Robotics Business Review*, 7 Mar 2018. https://www.roboticsbusinessreview.com/manufacturing/how-manufacturing-automation-is-evolving/

Further Reading

European Parliament. (2018). Civil law rules on robotics. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&from=EN

Jordan, J. (2016). *Robots*. Cambridge, MA: MIT Press.

S

SCADA

Marie-Helen Maras
Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Industrial control system · Critical infrastructure · SCADA

Definition

A supervisory control and data acquisition system (or SCADA) that monitors, controls, and otherwise supports critical infrastructure.

Introduction

An industrial control system is a general term used to describe "command and control networks and systems that are designed to support industrial processes" of critical infrastructure (ENISA n.d.). Critical infrastructure includes assets, systems, and facilities that are considered so vital to the United States that the incapacity or destruction of them would have a debilitating impact on society (Maras 2014, 2016). The focus of this entry is on one type of industrial control system, a supervisory control and data acquisition (or SCADA) system.

SCADA: In Brief

SCADA systems monitor, control, and otherwise support critical infrastructure. These systems "are highly distributed systems [and are used for remote monitoring and control over] geographically dispersed assets. They are used in distribution systems such as water distribution and wastewater collection systems, oil and gas pipelines, electrical power grids, and railway transportation systems" (Bobat et al. 2015, p. 2108; Stouffer et al. 2015, p. 2), among other areas. For example, in water distribution and wastewater collection systems and gas pipelines, they are used to monitor flow of water and pressure of gas in pipelines (Stouffer et al. 2015).

Vulnerabilities

SCADA systems are vulnerable to both physical threats (e.g., natural and human-made disasters, such as floods, fires, and even terrorism) and cybersecurity threats (e.g., unauthorized access or the exceeding of authorized access to systems). For instance, in 2000, Vitek Boden, a contractor for a company that installed the SCADA system for a sewage treatment facility in Australia, remotely hacked into the system and released

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

sewage near the facility (Maras 2014; Sayfayn and Madnick 2017).

There are special considerations for securing SCADA systems due to their design and functions (Stouffer et al. 2015). Because of their design and functions, SCADA systems are vulnerable to both remote unauthorized access through the channels used for their maintenance and the implantation of faulty data (which comprises the integrity of the data). In view of that, SCADA systems require strict access control features to prevent their unauthorized access and use.

There are several obstacles to securing SCADA. Given that some SCADA systems rely on proprietary operating systems, upgrades are not straightforward, and any changes to their operating systems need to be made by the vendors (Stouffer et al. 2015). In addition, "third-party security solutions [and support] are [often] not allowed [on such systems'] due to... vendor license and service agreements" (Stouffer et al. 2015, pp. 2–15). This is particularly problematic as vendor support may not be available when the support is needed, and service support may be lost if third-party applications are used and/or security solutions and/or support is obtained without prior agreement of the contracted vendor (Stouffer et al. 2015).

SCADA software and hardware applications are also more difficult to upgrade, and some systems may not have important security features, such as encryption (Stouffer et al. 2015). Unlike traditional information technology systems, software updates for SCADA systems, including security patches, are not applied in a timely manner (Stouffer et al. 2015). In fact, these updates are infrequent because vendors have to test these updates before implementing them – because of this, updates must be planned and scheduled well in advance (days and maybe even weeks in advance) (Stouffer et al. 2015). What is more, the components for these systems are also generally not easy to access and require a significant amount of effort to access them.

These challenges have led to "a significant transformation [of some industrial control systems] from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet" (ENISA n.d., para 2). This transformation, however, has brought about new vulnerabilities to cyberattacks (for more information about vulnerabilities to industrial control systems and critical infrastructure, see the *industrial control system* and *critical infrastructure* submissions in this encyclopedia, as well as the individual submissions for each of the 16 US critical infrastructure sectors: chemical; commercial; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems).

Conclusion

A SCADA system is a type of industrial control system. The protection efforts for SCADA systems must take the abovementioned special considerations and security obstacles into account to ensure that adequate protection is provided against both physical and cybersecurity threats.

Cross-References

- ▶ Critical Infrastructure: Commercial Facilities Sector
- ▶ Critical Infrastructure: Critical Manufacturing Sector
- ▶ Critical Infrastructure: Defense Industrial Base Sector
- ▶ Critical Infrastructure: Emergency Services Sector
- ▶ Critical Infrastructure: Government Facilities Sector (GFS)
- ▶ Critical Infrastructure: Nuclear Reactors, Materials, and Waste Sector
- ▶ Critical Infrastructure Protection
- ▶ Critical Infrastructure: Transportation Systems
- ▶ Critical Infrastructure: Water and Wastewater Systems Sector
- ▶ Industrial Control System

References

Bobat, A., Gezgin, T., & Aslan, H. (2015). The SCADA system applications in management of Yuvacik Dam and Reservoir. *Journal of Desalination and Water Treatment, 54*(8), 2108–2119.

ENISA. (n.d.). ICS SCADA. https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

Maras, M.-H. (2014). *Computer forensics: Cybercriminals, laws and evidence* (2nd ed.). Burlington: Jones and Bartlett.

Maras, M.-H. (2016). *Cybercriminology.* New York: Oxford University Press.

Sayfayn, N., & Madnick, S. (2017). *Cybersafety analysis of the Maroochy Shire sewage spill* (Working paper CISL# 2017-09 May 2017). http://web.mit.edu/smadnick/www/wp/2017-09.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). NIST special publication 800-82 revision 2. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Further Reading

Jaikaran, C. (2018). Cybersecurity: Selected issues for the 115th Congress. Congressional research service, R45127. https://fas.org/sgp/crs/misc/R45127.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). NIST special publication 800-82 revision 2. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Security: Concepts and Definitions

Clarissa Meerts
Faculty of Law, Department of Criminal Justice and Criminology, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Keywords

Security · Securitization · Public and private security

Definition

The measures taken to prevent, or respond to, criminal behavior.

Introduction

The concept of security literally refers to "a state of being free from danger or threat" (Oxford Dictionary). This is a very broad definition, and the word security is therefore used in different ways in different contexts. It may refer to a state of being free from many kinds of dangers and threats (e.g., war, unemployment, illness, or accidents). Some commentators have identified the fact that when security is used in this broad way, what is actually meant is *in*security (see, e.g., Schuilenburg and Van Steden 2014). In this context, it is important to point out the difference between "security from" (shielding from harm) and "security to" (enabling people to pursue their goals) (Crawford and Hutchinson 2016).

Security as a Contested Concept

Security as a concept is highly contested: there seems to be little agreement over its meaning (Crawford and Hutchinson 2016). Contributing to this situation is the existence of the closely connected concept of "safety." Safety also refers to a situation of being free from danger and risk but is more closely connected to physical conditions such as being free from injury. In practice, the difference between security and safety is commonly expressed as "safety" being about a situation of being free from physical harm or risk and "security" as being comprised of the measures taken to prevent, or respond to, criminal behavior. This is the definition used here. Security has, in this sense, moved away from being a state of being toward being a commodity.

Public Versus Private Security

Security provision can be organized by states (public security) or others (private security).

Sociologist Max Weber (1946) has famously stated that the monopoly over legitimate use of force is the essential tool of governance of states. In this view, security "is" public security. Taking a historical point of view, however, scholars such as Garland (2001) tell us that the monopoly of the state on security matters is an anomaly. In most of history, security provision has been a shared task of public and private actors, and the growing involvement of private actors in recent years indicates a move back toward that "normal" situation. One force driving the development of private security is the growth of mass private property in society (Shearing and Stenning 1981). (Semi-)public spaces (such as shopping malls and amusement parks) are often located on private property. This development fuels the growth of the domain of private security as well, simultaneously diminishing the domain of public police (Jones and Newburn 1993). In this way, security provision gets fragmented and divided among public and private actors.

Private security provision takes many different shapes. It can be about the provision of physical security (cash-in-transit, guarding of personnel or specific places such as an embassy, event, airport, the railway, maritime security, or a mall), of corporate and investigative services (such as employee theft or intelligence), of technical security services (such as alarm systems and camera surveillance and cybersecurity), or even of (para) military services. In addition to state-provided or private security, public/private partnerships and hybrid public/private entities have emerged (Jones and Newburn 2006).

Public Good or Private Commodity

As noted above, security is not exclusively provided by either the state or private parties. This fact has propelled an interesting debate that revolves around the question of the nature of security (Crawford and Hutchinson 2016). For some, security is a commodity which can be commercially traded and sold. Nodal perspectives on security tend to take this point of view, stating that we should view security as a commodity which is traded in the market, in which a multitude of (public and private) providers deliver security services. Security nodes provide security consumers with a choice, which is seen as a social good. The utilization of localized knowledge is regarded to make these security nodes more effective than state-provided security. The state is part of this complex of security nodes, but not prioritized over other security providers (Shearing 1992).

Others, also acknowledging the pluralistic nature of security, continue to see an essential role for the state. This is a result of their view that security is a public good, the provision of which cannot be left to the market (alone). The perspective of anchored pluralism concedes the fragmentation and pluralism of the market for security, while simultaneously prioritizing the state as a venue for security services over other actors (Loader and Walker 2006). Security is seen as a "thick" public good which consists of three dimensions. First, security is instrumental in the sense that it is a prerequisite for the enjoyment of – most notably – freedom. Second, security has a social dimension, in as far as the security of individuals is reliant in part on the security of others. And thirdly, security has a constitutive dimension: security helps constitute social cohesion and solidarity in a society. In the anchored pluralist view, security is not just about security (and safety) but also about justice – and the state is seen as the essential venue for that.

Governmentality and Securitization

The emphasis on security in contemporary society has been identified as "a culture of control" (Garland 2001) and as a securitization of society (e.g., Rose 1999; Schuilenburg 2015). In this context, the ideas of Michel Foucault are highly important. In his work about "governmentality", Foucault (1978) explains that security is used as a means to govern the population of a society. In this process, the state relies on other actors as well to be part of its "governance through

security agenda". Both the processes of securitization and the formation of a culture of control build on Foucault's ideas, referring to the situation in which security has become a dominant governing tool throughout society. Security has come to contain much more than reactions to crime, now also including undesirable behavior and disorder. It can even be said that security is the leading concept in society, guiding the way we think about a large diversity of subjects (Crawford and Hutchinson 2016). The scope of surveillance in contemporary society is unprecedented (Schuilenburg 2015).

Conclusion

Security is a contested concept. This is significant in the context of its importance for contemporary society. "Security" is omnipresent: as a mechanism to govern society, as an employer for many citizens, and as a substantial and ever-growing market for security consumers and providers. Whether security should be seen as a commodity or a public good, it impacts the everyday life of most citizens in modern society.

Cross-References

- ▶ Corporate Security
- ▶ Event Security
- ▶ Intelligence
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Video Surveillance, Equipment, and Training
- ▶ Public-Private Partnerships: Security Organizations
- ▶ Retail Security: Employee Theft

References

Crawford, A., & Hutchinson, S. (2016). The future(s) of security studies. *British Journal of Criminology, 56*, 1049–1076.

Foucault, M. (1978). Governmentality. In G. Burchell, C. Gorgon, & P. Miller (Eds.), *The Foucault effect; Studies in governmentality* (pp. 87–104). Chicago: The University of Chicago Press. (1991).

Garland, D. (2001). *The culture of control; Crime and social order in contemporary society.* Chicago: University of Chicago Press.

Jones, T., & Newburn, T. (1993). *Private security and public policing*. Oxford: Oxford University Press.

Jones, T., & Newburn, T. (2006). Understanding plural policing. In T. Jones & T. Newburn (Eds.), *Plural policing. A comparative perspective* (pp. 1–11). Abingdon: Routledge.

Loader, I., & Walker, N. (2006). Necessary virtues: The legitimate place of the state in the production of security. In J. Wood & B. Dupont (Eds.), *Democracy, society and the governance of security* (pp. 165–195). Cambridge: Cambridge University Press.

Rose, N. (1999). *Powers of freedom: Reframing political thought*. Cambridge: Cambridge University Press.

Schuilenburg, M. (2015). *The securitization of society. Crime, risk, and social order*. New York: New York University Press.

Schuilenburg, M., & Van Steden, R. (2014). Positive security. A theoretical framework. In M. Schuilenburg, R. van Steden, & B. Oude Breuil (Eds.), *Positive criminology. Reflections on care, belonging and security* (pp. 19–32). The Hague: Eleven International Publishing.

Shearing, C. D. (1992). The relation between public and private policing. *Crime and Justice, 15*, 399–434.

Shearing, C. D., & Stenning, P. C. (1981). Modern private security: Its growth and implications. *Crime and Justice, 3*, 193–245.

Weber, M. (1946). Politics as a vocation. In H. H. Gerth & C. Wright Mills (Eds.), *From Max Weber: Essays in sociology* (pp. 77–128). New York: Oxford University Press.

Further Reading

Beck, U. (1992). *Risk society: Towards a new modernity.* London: Sage.

Garland, D. (2001). *The culture of control; Crime and social order in contemporary society.* Chicago: University of Chicago Press.

Schuilenburg, M. (2015). *The securitization of society. Crime, risk, and social order*. New York: New York University Press.

Wood, J., & Dupont, B. (Eds.). *Democracy, society and the governance of security.* Cambridge: Cambridge University Press.

Wood, J., & Shearing, C. (2007). *Imagining security.* Devon: Willan Publishing.

Security: Contract

Anthony Gentile[1] and Lauren R. Shapiro[2]
[1]Security, Fire, and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA
[2]Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Outsourcing · Nonorganizational security · Physical security · Private security firms

Definition

Contract security refers to an organization that vends their security services for an organization that needs to protect their assets using physical security (manpower) with a degree of technology, if applicable.

Introduction

Most of the USA's critical infrastructure systems are privately owned and are protected using private security officers (Strom et al. 2010). Large and small businesses, residential housing, educational facilities, governmental agencies, and other segments of business may decide for a variety of reasons to outsource security by hiring a company or guards to protect employees, property, and customers. In fact, most chief security officers when surveyed by ASIS International (see Nemeth 2018, p. 129) indicated that they used contract security (63%) over in-house/proprietary (6%) or hybrid (31%) security. At the beginning of 2018, the total worldwide revenue generated by contract security firms exceeded 26 billion dollars (Perry 2018).

The company's or end users' decision to seek a contractual firm to provide security is often based upon the desired needs of an organization (Nixon and Kerr 2008). To make this determination, the company CEO should consider the following four questions:

- Does the decision maker have any in-house experience in the industry?
- Is that person someone in a leadership role who has knowledge of security applications?
- Is that person someone who can dedicate his/her time to oversee security?
- Does the firm have the resources (either monitory or staff) to self-employ?

These are just some of the questions which must be considered, and when answered in the negative, means that the firm should seek a contractual firm to provide security services rather than performing security for itself (i.e., proprietary security). This chapter will provide information regarding the benefits of contract security, as well as what companies should consider when deciding which contract security firm is best for their needs.

Benefits of Contract Security

The primary benefit of contract security is reduction in costs associated with recruitment, screening, and training of security personnel and in administration and operation overhead (Fischer et al. 2013; McCrie 2016). Secondary benefits include obtaining security that meets industry standards for expertise, distributing risk and legal liability toward vendor, and allowing end user risk managers to perform internal investigations and focus on information security (Fischer et al. 2013; McCrie 2016; Nixon and Kerr 2008).

Cost Benefits

One of the most overlooked benefits relative to cost is not that a contractual security service is in itself necessarily cheap, but rather the establishment of an hourly billing rate means that the company or end user can establish and manage its security budget for the year. Listed below are items which are packaged into the hourly cost of a security officer and, unless renegotiated during the term of the contact, remains fixed. Additionally, the end user hiring a contract

security organization or vendor can lower associated security costs because it will not be responsible for security equipment (e.g., patrol cars, uniforms, surveillance TVs) or personnel-related costs (Fischer et al. 2013).

Security Officer Payroll. In the industry, there is some controversy regarding whether contract security officers make less than those working for a proprietary organization. However, what is undeniable is within the agreed-upon billing rate, a variety of other costs are absorbed (Brownyard 2015). Inherent in any company's payroll are certain tax and associated burdens: items such as employer-mandated taxes, which include a portion of federal payroll tax (#941) and federal unemployment insurance (#940); applicable State Unemployment Insurance (SUI); as well as state mandated Worker's Comprehension Insurance and General Liability Insurance (see Averkamp 2019 for an explanation). The cost of employment benefits, including vacation time and mandated sick leave days (this mandate continues to pick up momentum as large cities such as New York and Los Angeles have implemented this employment regulation). Probably the greatest advantage to companies in terms of contracting security is unforeseen overtime. If a security officer is required to work past his/her regular hour limit and receives overtime, it is not the responsibility of the end user to compensate the security organization. The exception would be when the company requires overtime as a stipulation in the contract terms and agrees to pay for such service.

Training. Adequate training has to be an important aspect of any comprehensive security plan (Hertig and Davies 2011). The combination of experience and a thorough training program designed to improve the security officer's skills and knowledge are essential to a successful model. Some contractors have instructional training packages they offer to employees, increasing their own marketability (Hertig and Davies 2011). In most states, however, preemployment training is the responsibility of the candidate and not the cost burden of either the security firm or the end user (Nemeth 2018). Often a candidate will not qualify for employment without satisfying particular state-mandated preemployment training (Nemeth 2018). The exception for training cost to be shifted to the contractual firm is when specific training topics are a requirement of the end user. Items such as the use of access control technology, IT education, limits of and power of authority, to name a few, will most often become a cost to the contractual organization. Additionally, if the end user company at some point during the contract period seeks supplemental training, such as deportment, communication, or ethics and conduct, then this cost is often absorbed as well. Even state mandated "in-service" training can become an expense to the contractual organization (Nemeth 2018).

Administration and organization: Establishing an "in-house" (proprietary) security department requires the development, administration, and organization of a recruitment team, training programs, payroll staff, and the hiring of supervisory staff to include management (Nixon and Kerr 2008). There is little doubt that the administrative burden is significantly reduced when engaging with a contractual firm. All aspects of the hiring process are the responsibility of the vendor (Brownyard 2015). Items such as initial candidate screening, the interview process, reference checking, background review, state compliance review (when applicable), and preemployment drug screening shall all be tasks performed by the security company as part of its contractual obligation (Brownyard 2015). Along with the initial hiring phase, the vendor shall also be responsible to increase or replace the number of personal as needed or reduce the number of security officers for any reason (Brownyard 2015).

Supervisory personnel must also be part of the hiring process as direct supervision and oversight of all officers is the responsibility of the vendor. Proper management of site-specific duties, file maintenance, and incident report review are all functions that is the responsibility of the security firm (Brownyard 2015). Once staffing has been fulfilled and security training satisfied (see aforementioned training section), there is a financial obligation on the part of the contractual firm to

fund payroll on a weekly or biweekly basis. One of the quickest ways to create disgruntled, poorly performing, and overall dissatisfied security personnel in the contractual firm is to have systemic payroll problems, specifically, delays in the issuance of payroll, inaccurate payroll, or lack of funding resulting in payroll obligations to be unsatisfied. Any of these problems will undoubtedly lead to high turnover and cause a degree of confused and unsettled behaviors regarding proper staffing for the client.

File maintenance is another significant issue relevant to both contractual and proprietary organizations. Many states have mandates requiring that various documents be made available for review, in either the client file or employee jacket, for inspection by an authorized agent of a particular state. State-approved employment applications, copies of registration cards, proof of training, client contracts, and proof of insurance are just a few items many states require companies to have on hand. Contractual firms have a much better understanding of the applicable state rules and regulations as they deal with these issues more often than do any in-house security organizations.

Operational Benefits

Often considered the most significant value-added component of utilizing a contractual firm is its obligation to provide continuous service, even during the most extreme circumstances. The "back room" or dispatch center for a contractual firm is the heart beat of the organization as it must provide the client with security coverage even when regularly assigned officers call out sick, have scheduled time off, or simply do not show up for work. Fulfilling this contractual obligation proves costly as most times officers will be entitled to overtime pay while transferring between job sites (after completing his/her assignment). Once again, with very few exceptions, the contractual firm will not be entitled to charge the user company anything beyond the agreed-upon hourly rate, even though an added payroll burden was necessary to satisfy the contractual obligation of the vendor (Brownyard 2015).

The deployment of additional manpower during emergency situations would also be the responsibility of a dispatch center. As the cadre of officers in a mature organization would be greater than in a proprietary firm, the advantage of engaging a contractual firm is clear. The oversite and coordination of supervisory personnel is also the function of the operational team. The ability and requirement of supervisory personnel to visit a client venue is paramount to the success, satisfaction, and retention of the client. Often the function of the supervisor, as well as the on-site security officer, is written into the client contract, and the oversight of these duties is the responsibility of the contractual firm. Once again, this added value is of no additional charge to the client and embedded into the hourly billing rate.

Impartiality. In many cases, the contractual security officer can more readily, effectively, and without consequence enforce the rules and regulations provided by the user firm than a proprietary officer can (Hertig and Davies 2011). The general reasoning is that the contractual officer is employed by and paid by a firm other than the one to which he/she is assigned. The fact that the security officer has little, if any loyalty, to the user firm is of great advantage when enforcement of particular rules and regulations is required. Assignment rotation also discourages familiarity with in-house personnel and can be a useful tool against allowing unauthorized access of certain employees or the occasional breach of policies and procedures. If properly managed, this situation produces more consistency in the performance of job site duties.

Conclusion: Selecting a Security Vendor

There are few things in the business world that could replace experience. Selecting the proper security vendor for any company is of great importance and should be beyond the scope of cost alone. Items such as deliverables and positioning are two segments which must be considered and equally evaluated in the decision.

Deliverables. Deliverables refer to how the security vendor provides its service to the end user company. The items included are the type of technology based upon historical data, as well as levels of staffing based upon job site duties and requirements. Often assisting the client to define site-specific requirements and operational duties, then shaping these duties into easy-to-understand instructions is something that is enormously helpful to the user agency. Other areas such as reporting procedures, communication, planning, and performance audits all fall under the category of deliverables and should not be overlooked during the selection process. In particular, as end user companies do not have direct control over security matters, including disciplining officers who do not perform their duties, it is essential that they are able to communicate such issues and concerns to the contract firm.

Positioning. Positioning refers to the security firm's experience and service record. When deciding which contract firm is best for your company, you should ask the following questions:

- How experienced is the security firm in your segment of industry?
- Does the security firm currently provide service in this segment to other companies?
- Historically, is this a segment in which the security firm is considered an expert?

Many initial concerns are often eliminated simply due to the fact that the security firm is well-positioned in this segment and has the ability to anticipate certain problems. Assigning the best candidate with the most experience based upon recruitment and training to your location is easier due to the level of expertise the firm has in providing security in your field. Management and consulting are of great value as experienced leadership employees with the security firm help provide information as to which services should be promoted in favor of others. This is often an indication for where the segment is moving to and as to what to achieve in the future. Finally, the ability of the user firm to solicit advice and consultation from a firm with a degree of experience in a particular segment should provide a level of comfort knowing that suggestions and/or direction is being offered through experience and not based upon a best guess.

Cross-References

- ▶ Physical Security: Best Practices
- ▶ Security: Concepts and Definitions
- ▶ Security: Hybrid
- ▶ Security: Private

References

Averkamp, H. (2019). *Payroll withholdings: Taxes and benefits paid by employers*. https://www.accountingcoach.com/payroll-accounting/explanation/3. Accessed 12 Feb 2019.

Brownyard, T. (2015). The do's and don'ts of contract security. *Security, 52*(1), 24–26.

Fischer, R., Halibozek, E., & Walters, D. (2013). *Introduction to security* (9th ed.). Burlington: Butterworth-Heinemann.

Hertig, C. A., & Davies, S. J. (2011). Contract security training and development: Examining methods of contract training. *Security, 48*(4), 78–80.

McCrie, R. (2016). *Security operations management* (3rd ed.). Oxford: Butterworth Heinemann.

Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.

Nixon, W. B., & Kerr, K. M. (2008). *Background screening and investigations: Managing hiring risk from the HR and security perspectives*. Burlington: Butterworth-Heinemann.

Perry, R. H. (2018). *U.S. contract security industry* (10th ed.). https://www.roberthperry.com/uploads/2018_White_Paper1.pdf. Accessed 12 Feb 2019.

Strom, K., Berzofsky, M., Shook-Sa, B., Barrick, K., Daye, C., Horstmann, N., & Kinsey, S. (2010). *The private security industry: A review of the definitions, available data sources, and paths moving forward* (NCJ No. 232781). National Criminal Justice Reference Service website: https://www.ncjrs.gov/app/publications/abstract.aspx?ID=254874. Retrieved 12 Feb 2019.

Further Reading

Fay, J. (2011). *Contemporary security management* (3rd ed.). Burlington: Butterworth-Heinemann.

Sorrells, E. (2016). *Security litigation: Best practices for managing and preventing security-related lawsuits*. Amsterdam: Elsevier.

Security: Hybrid

Anthony Gentile[1] and Lauren R. Shapiro[2]
[1]Security, Fire, and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA
[2]Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords
Insourcing · Outsourcing · Organizational security · Nonorganizational security · Physical security · Private security firms

Definition

Hybrid security refers to the use of both contracted and proprietary security services to protect a company's assets.

Introduction

Businesses that have a need for security often inquire about security services that would be best suited to their organization (Nixon and Kerr 2008). Traditionally, businesses will choose from establishing a proprietary organization within their company (i.e., hire their own staff; McCrie 2016; Perry 2018; also see ▶ "Security: Proprietary" in this volume) or use a contract company (i.e., hire a security agency to provide staff; Fischer et al. 2013; McCrie 2016; also see ▶ "Security: Contract" in this volume) to satisfy their needs. As there are advantages and disadvantages to both proprietary and contract security services, the hybrid security model provides an excellent example of how the two types of services can be combined to give the company the best coverage (Nemeth 2018). When deciding between proprietary and contractual services, the company must consider cost, quality, and management needed to carry out both short-term and long-term security operations (Fischer et al. 2013; McCrie 2016). However, by employing a hybrid model of security, the company can maximize benefits and minimize difficulties typically provided by each. This chapter provides a review of each type of security model and describes the best use of the hybrid model.

Contractual Versus Proprietary Security

Contractual security service refers to security services that have been outsourced to a private or public entity in need of security services (Brownyard 2015). The security officers are recruited, screened, hired, properly trained, supervised, and managed by the contracted company (Nixon and Kerr 2008). Contractual security services are able to manage absences of personnel in an organized manner as they are flexible in terms of replacements and coverage, thereby providing a consistent presence at all posts with trained officers (Hertig and Davies 2011). When using contractual security service, the organization transfers their risk or liability to the contracted company meaning that any losses that are sustained during work are compensated by the contracted company through its insurance policy.

Proprietary security operations are those that are "in-house" or controlled entirely by the company, and these employees are loyal to the company (Sennewald 2011; Zalud 2007). Recruiting employees and providing administrative support are the tasks of the in-house organization, making operations financial costly, both in terms of hiring, payroll processes, and tax information needed for each security employee and in higher additional administrative and operational expenses (Nemeth 2018).

Whether using proprietary or contractual security services, the organization is responsible for providing all tools necessary in order to run a successful security operation, including cameras, monitoring systems, and other equipment. By establishing an internal security operation within the organization, the organizations directors can regulate policies and procedures for security staff (Zalud 2007). This allows them to maintain control over the policies and their enforcement (Nemeth 2018). The directors of the organization

know the location and facility better than most other individuals, allowing them to tailor their security needs (Reilly 2013; Zalud 2007). Outside agencies, in contrast, have the level of expertise needed to conduct security operations (Hertig and Davies 2011). By maintaining internal personnel, the organization can effectively control how their security staffs conduct their operations on day-to-day basis without any interference. The organization can also set its own requirements for experience, training, and other qualifications for its security personnel (Sennewald 2011; Zalud 2007). Contracted guards are subject to certain standards and requirements in order to work, whereas proprietary services can have a hard time determining what quality is or what the standard should be.

Conclusion: Benefits of Hybrid Security

Some of the complexities experienced between traditional security services can be related back to matters in management, cost, training, quality, administration, staffing, and expertise (Nemeth 2018). Most often businesses have only considered contract and proprietary security services as their two choices (McCrie 2016). However, the hybrid security model has gained momentum to user organizations as a flexible model for protecting assets. A hybrid security model can be an ideal service for any type of business as it blends both proprietary and contract security services (Nemeth 2018). Having a hybrid security model will allow a business to maintain an "in-house" management structure; a CSO or director of security, middle managers, and supervisors are generally all employed by the proprietary firm, allowing for complete oversight of all policies and procedures. Security officers are the responsibility of the contractual firm and report directly to the in-house management staff (Reilly 2013). One of the more significant values of this model to the user firm is that all human resource, administrative, and payroll issues stay with the contractual firm and they assume the burdens associated with these tasks (Sennewald 2011). Additionally, all operational issues are directly addressed in-house as management has the ability to maneuver personal at will without the permission of the contractual firm (Nemeth 2018).

Cost can be a consideration in the hybrid model as the proprietary firm employs security leadership to include midlevel managers (Sennewald 2011). Many firms in today's market are willing to assume the expense as a trade-off to complete oversight of their security operation (Nemeth 2018). Finally, it is of great importance should a firm elect to engage this model that the proprietary organization has a significant level of comfort with their contractual partners, both in terms of their ability to satisfy all of the obligations mentioned and the degree of expertise and guidance they bring to the user organization (Zalud 2007).

Cross-References

- ▶ Physical Security: Best Practices
- ▶ Security: Concepts and Definitions
- ▶ Security: Contract
- ▶ Security: Private
- ▶ Security: Proprietary

References

Brownyard, T. (2015). The do's and don'ts of contract security. *Security, 52*(1), 24–26.

Fischer, R., Halibozek, E., & Walters, D. (2013). *Introduction to security* (9th ed.). Burlington: Butterworth-Heinemann.

Hertig, C. A., & Davies, S. J. (2011). Contract security training and development: Examining methods of contract training. *Security, 48*(4), 78–80.

McCrie, R. (2016). *Security operations management* (3rd ed.). Oxford: Butterworth Heinemann.

Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.

Nixon, W. B., & Kerr, K. M. (2008). *Background screening and investigations: Managing hiring risk from the HR and security perspectives*. Burlington: Butterworth-Heinemann.

Perry, R. H. (2018). *U.S. contract security industry* (10th ed.). https://www.roberthperry.com/uploads/2018_White_Paper1.pdf. Accessed 2 Dec 2019.

Reilly, S. (2013). How to train your security training program. *Security, 50*(9), 122–124.

Sennewald, C. A. (2011). Career (proprietary) versus non-career (and contract) personnel. In C. A. Sennewald (Ed.), *Effective security management* (pp. 127–135). Burlington: Butterworth-Heinemann.

Zalud, B. (2007). Enterprise-wide alignment drives contract or proprietary decision. *Security, 44*(2), 46, 48–49, 52.

Further Reading

Fay, J. (2011). *Contemporary security management* (3rd ed.). Burlington: Butterworth-Heinemann.

Sorrells, E. (2016). *Security litigation: Best practices for managing and preventing security-related lawsuits*. Amsterdam: Elsevier.

Strom, K., Berzofsky, M., Shook-Sa, B., Barrick, K., Daye, C., Horstmann, N., & Kinsey, S. (2010). The private security industry: A review of the definitions, available data sources, and paths moving forward (NCJ No. 232781). Retrieved from National Criminal Justice Reference Service website: https://www.ncjrs.gov/app/publications/abstract.aspx?ID=254874. 2 Dec 2019.

Security: Private

Seungmug (Zech) Lee
Department of Criminology and Criminal Justice, The University of Texas at Arlington, Arlington, TX, USA

Keywords

Contract security · Law enforcement · Private security · Proprietary (in-house) security

Definition

Private security refers to the nongovernmental practice of protecting people, property, and information, conducting investigation, and safeguarding an organization's assets.

Introduction

Private security plays a role in protecting assets in both the public and private sectors. It means something different to the private sector, public sector, and public itself. Private security refers mainly to the use of interior and exterior measures to protect personnel and physical assets, such as access control doors, lighting in parking lots, or alarm systems. Others think of the people who safeguard assets and conduct investigations, specifically security officers, armored car drivers, or private investigators (see ▶ Private Detectives in this encyclopedia). Still, some others are concerned with cybersecurity, that is, protecting computer data, information systems, or data on the Internet.

Private security is a very large and vast field, comprised of the protection of lives and property in diverse ways, shapes, and forms. First, private security is a **nongovernmental** practice, indicating that protective services are produced by private individuals or private organizations. The origin of service products comes from private nature. In some cases, government agencies contract out part of their services with security companies, but still, the core security services and products are produced and provided by private hands. Second, services and products offered by private security are **fee-based** in case of contracted out practice. Any individual or governmental entity who needs security services pays with funds, which are either private money or public funds, to security professionals or companies. For the proprietary security arrangement, all operational cost comes from an individual or private corporate, not from public funds (see ▶ Security: Proprietary in this encyclopedia). Third, protective security services by private security are **contract-based** in case of contracted out arrangements (see ▶ Security: Contract in this encyclopedia). Unlike public police security services, where our society demands public fund-based, available 24/7, and permanent operations, security services are typically offered according to fixed temporary terms. Once it expires, the clientele can renew, terminate, or add/subtract the nature of the contract. Fourth, private security has **service-based** multifaceted aspects in its service and product.

There are other ways in which private security differs from public security. Public police are typically organized according to different governmental levels (e.g., municipality, county, state, federal, special districts, etc.) and primarily restricted to its own geographical jurisdictions. Private security, on the other hand, is based on a particular service the client is willing to purchase, which can be offered from other regions of the

USA or even from/to other countries. The client can even purchase private security services from multiple providers domestically and internationally. In this way, one security company is able to offer a variety of protective services and products (Cunningham et al. 1990; Fischer et al. 2019; Kakalik and Wildhorn 1971; Van Meter 1976).

In short, private security produces and provides protective services for life and property against hazards, including "natural" and "human-made" hazards. Examples of the natural hazards are fire, tornado, flood, earthquake, hurricane, blizzard, and other acts of nature which may result in disruptions or damage to the enterprise or organization, such as to cause building collapse, equipment failure, accidents, safety hazards, and other events that interrupt normal business processes. Examples of "human-made" hazards are crimes against the person (e.g., robbery, sexual crimes, etc.), crimes against property (theft, pilferage, fraud, embezzlement, etc.), as well as other problems, such as terrorism, espionage, sabotage, civil disturbances, bomb threats, workplace violence, cyber/Internet attacks. This entry discusses the historical development of private security, private security industry, issues regarding the roles of private security, and the future of private security.

History of Private Security

Private security has a long and sordid history. Much of the history of contemporary private security is intertwined with the history of policing. Both follow the shift and reform of legal foundations, taking the primary responsibility for protection and prevention of criminal activities from the private individual to the government. The history of private security germinates from a recurring inability of government sectors (Smith et al. 2017) and from a continual new challenge and threat to provide the level of security required by individuals and organizations.

The need for security can be traced back to the ancient world. Humans have always felt and practiced the need for security for both themselves and their possessions. Security practices and devices have been in existence for hundreds of years, dating back to 1500 BC. Two major security practices were dominated in the ancient world. First, the use of guards became popular at an early point in history, protecting persons and assets. Among the earliest examples of personal security professionals were those created in the thirteenth century BC when Egyptian Pharaoh Ramses II hired Nubians, Libyans, Syrians, and others to complement Egypt's military and native security forces. This practice continued in ancient Rome, where wealthy citizens often hired security professionals to protect their families and property. Augustus Caesar created three forces: the Praetorian Guard (as a form of bodyguard police), the Urban Cohorts (as a form of armed police, composed of soldiers with police and military duties), and the Vigiles (as a large body of police-fire fighters). This may well represent one of the first formal security forces in history (Collings et al. 2015; McCrie 2004, 2014; Smith et al. 2017).

Second, another common practice of the ancient world for protection and safety was to utilize physical security measures. For example, walls and barriers protected people and property by surrounding many cities in Europe and Asia, such as Rome, Troy, Constantinople, and the Great Wall of China. Ancient cities and palaces were surrounded by walls of great thickness and height. One such example was the Mycenaean fortresses with four zones of protection (layered defense lines) – the first line of defense with the use of water, the second line of defense with the outermost wall, the third line of defense with the wall surrounding the sacred precinct and palace, and the fourth line of defense (the final defense) with the wall of the building used as quarters for the royalty and their valuable possessions (Collings et al. 2015). This concept of sequential layers of defense lines has existed and practiced throughout all human civilizations and still applies in the twenty-first-century security operations management. Many of the developments and practices of the past are seen in today's security operations with the same goals: to keep others from accessing private property while providing individual and organizational security and protection. What has been changed is not the

fundamental principle of physical security but the asset to be protected and the technology to be implemented.

During the Middle Ages (from the fifth to the fifteenth century), security involved wealthy citizens building moats for protection of their property from potential intruders. While new policing reforms and practices had been implemented (such as tithings, shire reeve, constables, watch, ward, etc.), private police force emerged gradually to respond to new challenges. For example, by the mid-1600s, **thieftakers** acted as a private police force to capture and punish criminals. They were paid by the king for the conviction of criminals and rewarded for their efforts with the bounty of weapons, money, and property seized from the criminals they caught. They did not have any official status. By the mid-1700s in England, the **Bow Street Runners**, created and overseen by Henry and John Fieldings, acted similar to the thieftakers. There were no clear boundaries between public policing and private security until the first modern-era urban police department was established in London, UK, by Robert Peel in 1829 (Fischer et al. 2019; McCrie 2014; Smith et al. 2017). Ever since then, public police have dominated public safety and protection roles, while private security has focused its roles of protection and safety on more private individuals and private corporate business and assets. Two distinct paths toward protection and prevention between public police and private security were paved.

In the North American context, private security has excelled during the late 1800s beginning from the Pinkerton National Detective Agency in 1850. The so-called original big three, Pinkerton in 1855, Brinks in 1859, and Burns in 1909, started their private security business by providing investigation, guarding, as well as freight and package delivery. In 1850, Wells Fargo offered a freight transportation service. Then Holmes in 1858 and ADT (American District Telegraph) in 1874 both began providing alarm installation and response services (Fischer et al. 2019).

Another noticeable development between the mid-1800s and early 1990s was railroad police. As the USA expanded westward, railroad lines in the new territories received little or no coverage of protection and safety from public police. Local outlaws robbed passengers, stole cargo, dynamited tracks, and disrupted communications. Numerous state legislatures passed railroad police acts for railroad companies to establish their own security forces with full police powers in response to demands for adequate protection of goods and passengers. By 1914, there were over 14,000 railway police in the USA. In addition, steamship lines, banks, factories, mines, and retail establishments employed more and more private security professionals (Smith et al. 2017).

World War I and II became a catalyst for private security to expand its roles and activities. The use of private security increased not only because of urbanization and industrial growth but also to protect government assets against sabotage and espionage. For example, during World War II, more than 200,000 plant watchmen were given special auxiliary military police status to protect products, supplies, equipment, and personnel. The 1960s' social unrest and 1970s' sudden increase of crime rates across the nation played a critical role in the growth of private security. By the mid-1900s, many private security companies had joined the ranks (Fischer et al. 2019; Smith et al. 2017). Today, the protection and safety of our nation and our communities is a shared responsibility between public police and private security sectors. Private security is the primary resource for individual and property protection.

Private Security Operational Types and Activities

Operational management of private security services has three types: contract security, proprietary (in-house) security, and hybrid security. **Contract security** companies offer protective services for a fee to people, agencies, and companies which do not employ their own security personnel or which need extra protection. Contract security professionals are generally not peace officers with police power. In 2013, there were nearly 10,000 such companies in the USA (Fischer et al. 2019; Smith et al. 2017). Early researchers perceived more rapid growth in contract security operations

than in in-house security type, and the trend has been toward increased use of contract security professionals, products, and services. Some advantages with contract security type include cost saving, dealing with less administrative issues (e.g., recruitment program, training program, scheduling, substituting manpower, etc.), flexible staffing (e.g., laying off, taking on additional staff, or emergency use), more nonunion security professionals (i.e., only a fraction of security officers are unionized), more impartial performance of duty, and customized security services (Fischer et al. 2019).

On the other hand, proprietary (also called as in-house security) operations provide protective services for the entity and are controlled by the company. They are also not classified as sworn peace officers. About 40% of all private security officers are in a proprietary arrangement. Most of them are employed in retail/restaurants/food services (16.7%), casinos/hospitality/arenas/entertainment (15.7%), health care/medical centers/hospitals (12.9%), and government (10.9%) (Smith et al. 2017). Several advantages of in-house security operation include higher quality of security personnel, more careful employ screening processes, lower rate of turnover, greater degree of control over security personnel, loyalty, and increased prestige by building the company's own security force (Fischer et al. 2019).

The third type of security operations is hybrid systems, combining both in-house and contract security functions (see ▶ Security: Hybrid in this encyclopedia). The final arrangement among different types varies depending on the nature, location, and size of the firm. Primarily for cost reason, the number of contract security jobs is likely to increase faster than that of in-house security jobs. BLS projects employment of security guards grows by 5% between 2014 and 2024, which is about average for all occupations (Smith et al. 2017).

Whatever actual types of security operations there may be, there are still several common security functions performed by security professionals, which can break down into four main components – physical security, fire and emergency managements, information/data protection, and enforcement of rules and policies. **Physical security** functions include building and perimeter protection, intrusion and access control, and alarm and surveillance systems. **Fire and emergency managements** are related to fire prevention and control, emergency response, crisis management, and disaster recovery planning. **Information/data protection** functions are done by protection of intellectual property/data/information systems. **Enforcement of rules and policies** is operated by regulating and applying crime- or loss-related rules and policies, implementing preventive regulations of theft and pilferage and workplace violence.

Private Security Industry and Factors for Growth

The private security industry has grown tremendously since the 1970s. It is a huge enterprise that produces security hardware and provides protection services. There are between 11,000 and 15,000 such companies (not including in-house security operations) in the USA, compared to about 18,000 public law enforcement agencies, but there are more people working in the private security sector. For example, in 2016, over 1.13 million people worked as security guards and gaming surveillance officers, while about 800,000 people worked in public police (Bureau of Labor Statistics (BLS) 2019). Major categories of services private security industry provide are security forces, patrols, consulting services, investigative services, alarm response, armored car delivery and courier services, executive protection, and event security.

There are three reasons for the increased use of private security industry. First, during the last two decades, virtually all major cities and state governments in the USA have experienced severe budgetary cutbacks. Public police agencies have gone through their share of across-the-board government funding reductions, resulting in limitations and even freezing on the hiring of additional police officers. Police departments have also curtailed services, leading to an increase in the use of private security professionals and companies to fill the gap in protective services.

Second, a business depends on a positive reputation to remain competitive. Widespread employee theft, embezzlement scandals, and substance abuse all harm a private company's public image and may cause potential customers to question the quality of its products and services. By employing in-house security professionals or contracting out, companies may implement preventative programs and handle internal criminal cases.

Third, by employing in-house security personnel or by contracting out with outside security companies, management in the private sector can direct security professionals to do precisely what is needed to prevent crime, minimize substance abuse, and discipline wayward employees. It should be noted that private security employees are typically male and white. In 2015, security guards and gaming surveillance officers were 78% male, 29% black, 19% Hispanic, and 4% Asian (Bohm and Haley 2018; Smith et al. 2017). Security guards generally receive relatively low wages, typically working 8-hour shifts, 5 days a week. Because of relatively low wages, private security officers frequently work part time or have another "primary" job and use their security job wages to supplement their incomes.

Issues of Private Security

Several unresolved problems and issues have been raised on the potential for further positive developments and roles of private security. First, legal status and authority of private security officers in many circumstances are not clearly understood, mainly because historically they derive from the rights of the owner/landlord who deputize security officers to protect property on the premises. Public police derive their rights and authority to act from a variety of statutes, court cases, ordinances, and orders enacted at various levels of government, are subject to public scrutiny, and have substantially greater powers than do security officers to arrest, detain, search, and interrogate (Bohm and Haley 2018; Fischer et al. 2019). But private security officers act essentially as private citizens, facing few constitutional limitations in their activities and being limited to the premises of their employer (see ▶ Security Guards: Authority and Power in this encyclopedia).

A second issue concerns security personnel's qualifications and training. Although many highly qualified individuals work in private security at all levels, they are not the norm. Private security fields and governments have attempted to regulate the private security industry and to increase the minimum qualifications for their officers, but security fields lag far behind those of the public police. All but five states –Colorado, Idaho, Mississippi, Missouri, and South Dakota – require that either private security companies or private security officers be licensed in some manner. In three of the states without licensing requirements – Colorado, Idaho, and Missouri – their largest cities, St. Louis in Missouri, Boise in Idaho, and Denver in Colorado, require security guards to be licensed (Nalla and Crichlow 2017). Though the majority of states require legal status in the USA (either US citizen or permanent resident), the minimum age for unarmed guards is 18 years old, and for armed guards, it is 21 years old; the minimum education level is at least a high school diploma or equivalent, and the minimum of formal training is at least 8 hours. Some large private security companies (such as Securitas and Wackenhut) have more minimum training requirements than what the states require in which they operate. The qualifications of proprietary security officers are generally higher than those of contract security officers, demonstrating that corporate is willing to pay a good salary in exchange for high-quality security services (Fischer et al. 2019).

A third issue is related to diminished public responsibility. The current cooperation of public and private protection is a matter of concern to many Americans (Bohm and Haley 2018). Some concern that since private security sectors have greatly expanded their protective services and roles, it seems that public police officers and the governments shift responsibility for protecting life and property to private security enterprises and default on a major portion of the social contract for domestic safety and protection. Still,

others concern the extent of roles and responsibility that private security can contribute.

A fourth issue concerns public policing in a private capacity. Many police departments prohibit moonlighting, but thousands of police officers still work in a private capacity during their off-duty hours with police uniforms and firearms. Some police agencies even cooperate with private agencies in scheduling their officers for off-duty assignments. One serious legal question with such an arrangement is whether these moonlighting officers are considered public police or private security officers. Another equally important question is who is liable if moonlighting officers abuse their authority or make a mistake (Bohm and Haley 2018).

Conclusion: The Future of Private Security

Growth in private security is shown by an increase in expenditures, employment numbers, and value of the equipment. Many new firms have entered security and protection business, established firms are showing strong growth, and some Fortune 500 companies and foreign firms are buying security companies. In a time when public law enforcement is experiencing little or no growth, private security directors are experiencing greater demands on their resources and professional expertise. The private sector has a tremendous impact on crime and the criminal justice system. The private sector will bear more of the burden for crime prevention and asset protection, while public law enforcement will narrow the focus of police services on crime control.

Both private security and public police need each other in order to be successful in sharing the crime prevention burden while protecting citizens, shareholders, and employees of a business. Interaction and cooperation between these two sectors are getting more critical and vital. Professional organizations representing private security would approach colleges, universities, and community colleges and ask for help with programs that train security officers and security professionals. More certification and education programs will be developed and offered due to increased demand for training and education for security officers.

Technological advances in security, including integration of computer and biometrics with CCTV (closed-circuit television) and access control protocols, should improve protection of assets. The combinations of biometric, electronic, and computer technologies in a layered approach will provide security and other management personnel to have effective and efficient surveillance. Integration of security technology is a continuing process to equip security guards and managers with smart cameras and wireless technology to provide real-time updates. Private security is increasingly becoming global, providing opportunities for security professionals. Private security is impressively optimistic and lucrative for the motivated person with a sound educational preparation, certification, and training (Fischer et al. 2019).

A variety of threats, such as active shooters and disasters, as well as natural hazards and man-made disasters, are constant challenges for security professionals. Active shooter situations that have become far too commonplace and the issue are complicated by the politics of gun control versus the Second Amendment in the US Constitution. Similarly, terrorism is another threat to both public police and private security. Since the 9/11 attacks, the private security industry and its officers have been given more protection responsibilities as the threat of domestic terrorism in the USA has increased (Fischer et al. 2019).

Private security officers are often the first line of defense against various emergency situations, criminal activities, terrorist attacks, and natural disasters in the USA and other nations. Limitations of the criminal justice system have been recognized, and the resultant void is being filled with some success by the private sector. The public sector cannot afford to pay for all of the protection needed in our modern and turbulent world. One formidable approach of providing protection and security is through the use of private resources that keep the costs of products down and provide an environment wherein our democracy and free enterprise system with social responsibility can be protected and progress.

Cross-References

- ▶ Private Detectives
- ▶ Security: Contract
- ▶ Security: Hybrid
- ▶ Security: Proprietary
- ▶ Security Guards: Authority and Power

References

Bohm, R. M., & Haley, K. N. (2018). *Introduction to criminal justice* (9th ed.). New York: McGraw-Hill Education.

Bureau of Labor Statistics (BLS). (2019). *Occupational outlook handbook*. Washington, D.C.: U.S. Department of Labor, Bureau of Labor Statistics.

Collings, P. A., Ricks, T. A., & Van Meter, C. W. (2015). *Principles of security and crime prevention* (4th ed.). New York: Routledge.

Cunningham, W., Strauchs, J. J., & Van Meter, C. W. (1990). *The Hallcrest report II: Private security trends 1970–2000*. Boston: Butterworth-Heinemann.

Fischer, R. J., Halibozek, E. P., & Walters, D. C. (2019). *Introduction to security* (10th ed.). Cambridge, MA: Butterworth-Heinemann.

Kakalik, J. S., & Wildhorn, S. (1971). *Private police in the United States: Findings and recommendations*. Santa Monica: The RAND Corporation.

McCrie, R. D. (2004). The history of expertise in security management practice and litigation. *Security Journal, 17*(3), 11–19.

McCrie, R. D. (2014). A history of security. In: M. Gill (Ed.), The handbook of security (2nd ed.) (pg. 21–43). London: Palgrave Macmillan.

McCrie, R. D. (2016). *Security operations management* (3rd ed.). Waltham: Butterworth-Hernemann.

Van Meter, C. W. (1976). *Private security: Report of the task force on private security*. Washington, D.C.: National Advisory Committee on Criminal Justice Standards and Goals.

Nalla, M. K., & Crichlow, V. J. (2017). Have the standards for private security guards become more stringent in the post-9/11 era? An assessment of security guard regulations in the U.S. from 1982 to 2010. *Security Journal, 30*(2), 523–537.

Smith, C. F., Schmalleger, F., & Siegel, L. J. (2017). *Private security today*. Boston: Pearson.

Strom, K., Berzofsky, M., Shook-Sa, B., Barrick, K., Daye, C., Horstmann, N., & Kinsey, S. (2011). *The private security industry: A review of the definitions, available data sources, and paths moving forward*. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics.

Further Reading

Purpura, P. (2018). *Security and loss prevention* (7th ed.). Waltham: Butterworth-Hernemann.

van Steden, R., & Sarre, R. (2007). The growth of private security: Trends in the European Union. *Security Journal, 20*, 222–235.

Security: Proprietary

Anthony Gentile[1] and Lauren R. Shapiro[2]

[1]Security, Fire, and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA

[2]Department of Security, Fire, and Emergency Management, John Jay College of Criminal Justice, City University of New York, New York, NY, USA

Keywords

Insourcing · Organizational security · Physical security · Private security

Definition

Proprietary security refers to in-house security services, including physical, information, and employment-related protection of assets and personnel, provided by the company to itself through employees that it hires, manages, and trains (Nemeth 2018; Strom et al. 2010).

Introduction

Approximately 20 billion dollars are spent annually by firms across the world in a variety of sizes and segments who choose to develop and provide security as a proprietary or in-house function (Perry 2018). Often this decision is based upon the desire to have more control over the entire security operation and has much appeal to organizations that value loyalty, quality, and prestige of their security staff while eliminating the large rate of employee turnover often associated with a contractual security firm (McCrie 2016).

Where and how the proprietary security organization functions within the organization is a matter of great importance and shall determine its value and strength. There is clearly a thought process that suggests a proprietary security model is more expensive than a contractual model (i.e., outsourcing security; see ▶ "Security: Contract" in this encyclopedia); therefore, how it functions both operationally and financially has considerable significance. Unlike with the contractual model, there must be a designated security leader in the proprietary model whose function shall be to carry out security policy and procedures (Nemeth 2018). The degree and level of authority that the head of security (often a C suite position) or chief security officer (CSO) shall have will depend upon the level of need, importance, and vision the organizations' senior leadership has as it relates to the value safety and security it has to the overall organization as it continues to grow (Brennan and Mattice 2014; Finch 2013).

It is therefore incumbent upon senior leadership to establish goals and objectives properly which the in-house security organization shall be guided by to properly control spending while enjoying the best security outcomes (ASIS International 2012 as cited in Nemeth 2018). The CSO is held directly responsible for the performance of the in-house security department and must ensure his/her operation contributes to the overall asset protection model (see ▶ "Physical Security: Best Practices" in this encyclopedia). A strong synergy with the human resource department is valued as most recruiting, vetting, selecting, and hiring are handled in-house and through this department. Often state-mandated training and site-specific training shall be the direct responsibility of the security department (Reilly 2013). For large companies, interfacing with legal is also an important aspect of a proprietary security department.

Benefits of Proprietary Security

The obvious main benefit to proprietary security is control over personnel as the company handles its own recruitment, selection, training, and management (McCrie 2016; Reilly 2013). Secondarily, the benefits are that the highly qualified, career-oriented personnel are familiar with the specific needs of the company, are available on a consistent basis, and, as a result of receiving good pay and benefits, will be loyal to the company (Sennewald 2011; Strom et al. 2010).

Level of Employee Quality

According to Sennewald (2011), companies which have proprietary security are able to recruit personnel who seek careers, rather than merely jobs. Arguably the quality of an employee is determined, to some degree, by his/her rate of pay. In most cases, the proprietary organization has the ability to provide security personnel a highly competitive position by offering:

> salary, pension or retirement plans, profit sharing programs, the entire employee 'benefit package' (which usually includes medical, hospitalization, dental and life insurance, vacation, and sick leave), and employee privileges unique to the company (such as merchandise discounts in retailing and free or near-free travel for those in the transportation industry). (Sennewald 2011, p. 128).

The company, in turn, benefits by being able to hire a good-quality candidate, both in terms of the person's experience and education (Zalud 2007). Moreover, the proprietary security personnel are vested in the company, making them both ambitious and motivated to remain with the employer as they work toward promotion (Nemeth 2018; Sennewald 2011). As a result, the company has a stable and consistent work force, in whom it can invest time and resources knowing that improvement in security performance combined with dedication to the company will be the results (Sennewald 2011). The proprietary security personnel are technically proficient and share a comradery with the other employees. Reducing employee turnover is considered an asset to the company as the employment search process and training process are costly and time-consuming both to HR and to the security department (Reilly 2013; see ▶ "Security Guards: Academic and Training Programs" in this encyclopedia). The

organization treats members of the security department as it would any other employee, which allows security team members to have the feeling of belonging, something often absent in the mindset of a contractual employee (Zalud 2007; also see ▶ "Security: Private" and ▶ "Security: Hybrid" in this encyclopedia).

Control and Supervision

Being in direct control of security personnel is a significant advantage in the propriety model as the security manager and senior leaders in the company have dominion. Communication between the security personnel and the rest of the company employees is typically better because all of them share in common a mutual company identity and set of interests (Sennewald 2011).

The corporate security officer (CSO) is an essential member of the executive team, all of whom operate under the same mission to grow the company (Nemeth 2018). Unlike contractual security, the CSO of in-house security department will have a greater degree of control and supervision over employees (Zalud 2007). In particular, the CSOs and security managers are able to message the security team directly and quickly regarding the rollout of new or amended jobsite duties, change in security direction, a disciplinary concern, or simply a special one-time requirement. This streamlined approach is clearly a time-saver as the same message when contract security personnel are used would need to first go through that organization prior to getting filtered down to the applicable officer(s) for implementation. Additionally, in-house security managers are able to perform the necessary task of daily supervision of the security staff, allowing them to make immediate corrective action should a violation be detected (Nemeth 2018). In a contractual model, staff violations would often first be reported to a central location for determination, which is time-consuming and does not allow for adjustments to be made at the point of concern in a timely manner. The CSO must also oversee a program that will teach its security personnel about risk evaluation and security training at hire and periodically afterward to maintain a high standard of competence and upgrade their skills (Reilly 2013). Although organizations using a contract agency can include verbiage in their contract to allow them to remove guards, it is not a common practice.

Loyalty

Employees who enjoy longevity in their tenure with a company are often also loyal to it; this same philosophy can be applied to proprietary security personnel. The security team identifies with other employees in the company, and all of them will feel pride and self-admiration when the business grows and succeeds as a direct result of their dedication and hard work. The level of reliance placed upon proprietary officers to perform their duties is often heightened due to the level of familiarity with the organization and how the business model functions (Zalud 2007). These employees are integrated into the company's culture and value system, accepted as members of the group, and included in business functions, such as holiday parties and other celebrations. This type of treatment fosters a great sense of belonging as proprietary security are looked upon as equal members, that is, like any other employee in the firm (Sennewald 2011). In this way, the CSO is able to gain the team's acceptance, support, and compliance in security-related matters for the company, actively involved in supporting company interests (Nemeth 2018). The CSO will also give preferential treatment of the security officers since as a team they provide protective services to assets and personnel. They may be given a higher level of consideration when requesting compensation and time off because they are expected to assume a great deal of responsibility and have earned the respect of the company. With a contractual firm, longevity of personnel at their jobsites is atypical and often only occurs with the most determined and dedicated employees. Due to salary disputes, transportation issues, level of responsibility, and shift assignments, turnover can and often will affect contract security employees' length of stay at any one venue. Hence, these officers are absent of loyalty because they simply do not have any feeling of value to the jobsite other than the proper

performance of their duties (Sennewald 2011). Some security professionals consider the disconnect between employment and loyalty the most considerable contrast between the proprietary and contractual models and often one of the major considerations when deciding on which security business model best fits the needs of the organization.

Prestige

Many CSOs or corporate senior leaders prefer to have their own in-house security team in place because they believe it gives their organization a level of admiration and prestige. Secondarily, they believe developing a unique and specialized security system (both physical and technological) for the sole purpose of protecting the people and property of their organization is necessary (Nemeth 2018). In a conceptual sense, there is clearly an underlying thought that an in-house security department is more highly regarded and run with a greater degree of professionalism than could be offered by a contractual firm (see ►"Maritime Security: Armed Guards on Board" in this encyclopedia). The downside of this model is a considerable increase in spending, compared to the stable and known expenditures of contractual security, which may be overlooked in the organization's goal to project an optimum level of status.

A sense of prestige and importance also becomes embedded within the security office. Working for a well-known and globally recognized organization is clearly more prestigious and seemingly more important than working for an unknown security firm (see ►"Security: Contract" in this encyclopedia). The fact that a uniform displays the name of this well-known organization rather than that of a nondescript company may be a source of pride for security officers. In particular, when those in the security industry have the opportunity to congregate and discuss their employment, a boastful tone may be associated with certain firms and locations over others. This sense of pride should not be dismissed as it leads to employment longevity, a significant degree of caring and ownership that the work is impactful, and provides security officers with a sense of importance.

Financial Impact

Arguably the proprietary security model is more costly than the contractual security model as the in-house firm is responsible for all HR-related issues. Specifically, the proprietary organization is responsible for screening and vetting, training, supervising, and managing the officers and providing security-related equipment (Sennewald 2011). Conversely, the degree of loyalty expressed and the feeling of prestige felt by security officers often bring with it a high degree of retention, reducing the significant level of turnover often associated with the security industry (Zalud 2007). This might not balance out the additional expenditures with this model, but clearly retention becomes a cost-saving tool that allows many firms to continue to use an in-house team. Other items, such as payroll-related taxes (federal, state, local along with unemployment taxes), uniform expense, overtime cost, vacation allowance, and in-service training, all become the burden of the proprietary organization (Nemeth 2018).

But often the largest financial burden an in-house organization must cover is that of liability and personal injury exposure. In the proprietary model, the company is susceptible to a variety of liability risks during the performance of security officers' daily routines. Items such as errors and omission, personal injury, false arrest, assault, and battery and property damage all become the responsibility of the in-house firm, should security officers make egregious errors while performing their job site duties (Nemeth 2018). Additionally, workers' compensation insurance (unlike liability insurance, WCI is generally required in all states) provides benefits to employees for work-related injuries or illnesses, which include medical care, wages due to lost work time, and benefits to families of deceased workers as well (Nemeth 2018). Accompanied with providing liability and workers' compensation coverage comes the added risk of increased premiums, should the firm experience exposure to one or both of these necessary forms of insurance coverage, such as

when a claim requires the underwriting insurance company to provide monetary satisfaction.

Conclusion

Ultimately senior management of the proprietary organization will have to determine if the potential increase in effectiveness and efficiency is outweighed by the projected additional financial burden of providing an in-house security unit. Evaluating the need(s) to expand as the organization grows both in size of employees, and expansion of their facility must also be a strong consideration. Management must recognize that security-related concerns, either real or potential, often require the expansion or enlargement of the security operation, but associated costs should not influence this decision. Finally, and often overlooked in this model, is that many states do not require a significant level of oversight to an in-house security operation. Regulatory concerns, such as hiring someone who holds a particular state security license, are typical of contractual security which vends its service to others (Strom et al. 2010). Simply registering your firm as an in-house security operation with the applicable state is usually sufficient. Furthermore, security officers in some states do not need to register with the applicable licensing body or go through any level of mandated training, streamlining the hiring process (see ► "Maritime Security: Armed Guards on Board" in this encyclopedia). Proprietary organizations must decide what level on screening and training shall be considered adequate.

Cross-References

- ► Physical Security: Best Practices
- ► Security Guards: Academic and Training Programs
- ► Security: Contract
- ► Security: Hybrid
- ► Security: Private

References

Brennan, J., & Mattice, L. (2014). Managing risk across enterprise. *Security, 51*(7), 22.

Finch, B. (2013). The security leader, the business leader. *Security Magazine, 50 (6)*, 20–22, 24.

McCrie, R. (2016). *Security operations management* (3rd ed.). Oxford: Butterworth Heinemann.

Nemeth, C. P. (2018). *Private security: An introduction to principles and practice*. Boca Raton: CRC Press.

Perry, R. H. (2018). U.S. contract security industry (10th ed.). Accessed at: https://www.roberthperry.com/uploads/2018_White_Paper1.pdf. 2 Dec 2019.

Reilly, S. (2013). How to train your security training program. *Security, 50*(9), 122–124.

Sennewald, C. A. (2011). Career (proprietary) versus non-career (and contract) personnel. In C. A. Sennewald (Ed.), *Effective security management* (pp. 127–135). Burlington: Butterworth-Heinemann.

Strom, K., Berzofsky, M., Shook-Sa, B., Barrick, K., Daye, C., Horstmann, N., & Kinsey, S. (2010). The private security industry: A review of the definitions, available data sources, and paths moving forward (NCJ No. 232781). Retrieved from National Criminal Justice Reference Service website: https://www.ncjrs.gov/app/publications/abstract.aspx?ID= 254874. 2 Dec 2019.

Zalud, B. (2007). Enterprise-wide alignment drives contract or proprietary decision. *Security, 44*(2), 46, 48–49, 52.

Further Reading

Fay, J. (2011). *Contemporary security management* (3rd ed.). Burlington: Butterworth-Heinemann.

Sorrells, E. (2016). *Security litigation: Best practices for managing and preventing security-related lawsuits*. Amsterdam: Elsevier.

Security: Theories

Veronika Nagy
Willem Pompe Institute for Criminal Law and Criminology, Utrecht University, Utrecht, The Netherlands

Keywords

Security · Theory · Realism · Neorealism · Securitisation · Critical · Security dilemma · Constructivism · Liberalism · Feminism · Copenhagen School · Paris school · Power

What Is Security Theory? – The Definition

Security theories are perspectives on security, based on different epistemic backgrounds.

What Is the Core Concept of Security?

Though an average citizen usually thinks first about security in terms of social and public security, when we discuss the meaning of the concept in theoretical terms, security has its own meaning in different disciplines. Though some features are definitely common with social security or issues applied to various law enforcement problems, in Security Studies, the core subject of it seeks to explain and to identify the causes and to anticipate the likely consequences of events considered as a security issue (Collins 2016). While social security is generally linked to the internal order of social coexistence (to guarantee life, wealth, and rights of the individual), public security, job security or social justice, the concept in security theories, is rooted in the traditions of politicization. Before we turn to specific examples of security theories, it is necessary to introduce the most important concepts that have influenced security studies development.

Introduction

Originally, the term "security" itself (as did the German "die Sicherheit" or the French "Securité") comes from the Latin words "sine cura," which mean "without danger" or "without threat" (Gazdag 2011: 11). After its widespread use in the late 1940s, the word 'security,' regardless of its complexity, established a narrow definition in international security studies as a sub-area of international relations. The original term implies a negative approach that makes security equal to the absence of danger and threat. However, other approaches emphasize a positive definition of security, thus emphasizing the existence of factors that contribute to maintaining or establishing security. The term security was originally defined as a set of political goals, strategies, and tools that serve to prevent war while maintaining the ability for political self-determination. Its objectives are "to protect the political independence, territorial integrity and economic viability of the State, to ensure the security of its citizens and the development of their personalities." (Ritch 2001: 33). It should be noted, however, that security studies are not the same as strategic studies, which mainly deal with the use of armed force, and, therefore, it covers a much narrower area than security studies (Colins and Cohen 2007). The use of definition here corresponds to the Anglo-Saxon scientific discipline.

According to the collections edited by Collins, Ian Bellamy defines security as "relative freedom from war"; Walter Lippmann thought of security as a situation in which the nation does not have to sacrifice its key interests; However, Arnold Wolfers defines security in economic, cultural, and moral terms and considers it as a lack of fear, in terms of fear that aquired values would be at risk. Also, in Ken Booth's definition, security is interpreted as the freedom of people to do whatever they want without any physical or human compulsion. From all this "definition clutter," it can be seen how difficult it is to formulate what it means. Instead of choosing one of the definitions, it is advisable to accept the heterogeneity of the area and emphasize the inherently versatile nature of the concept of security.

Looking broadly, security theories deal with how to ensure the security of individual entities, the security of a nation, considered as the most important guarantee of which is the state. In our globalized world, this may seem anachronistic, but states are still considered as the key players in an international strategic environment. Shortly, security theories provide scenarios for how political actors' work can affect the security of an entity. The entity to be provided called the "reference object" might be interpreted on several levels: for example, cities, regions, nations, states, the international system, or even the security of the entire planet. Hence, the limitations considering the objectivities and conceptual framework of security studies are still a highly debated issue.

It should be emphasized that the concept of security has radically widened in the last decennia, broadening from purely military to a more general formulation. Currently, there is no sharp distinction between domestic and international security, and the boundaries of external and internal security are often blurry, especially due to increasing amount of non-state actors such as corporates and NGOs engaged in security field today. Security theories thus explain through abstract models how to ensure the security of some reference objects, such as a nation, and like most theories, address the question about how our reality works and how to define the impact of security issues to reality. Furthermore, most theories also give normative guidance to the actors on how to handle the various specific procedures in this reality (Baldwin 1997).

Recent Security theories are shaped by several disciplines including social sciences, political science, economy, and policing studies. As a subfield of international studies, Security studies is established after the First World War, following the establishment of the Department of International Politics at Aberystwyth University, United Kingdom (Williams 2012). As an independent scientific discipline, it only appeared after World War II, with some major achievements related to the appearance of nuclear weapons and the possibility of an outbreak of a thermonuclear war. Such changes increased the recruitment of civilian advisors in foreign and security policy, an area previously dominated by military personnel, also thanks to the recognition of the need to exercise civil and political control over nuclear power (Buzan and Wæver 2007). These developments shaped several epistemic schools in security theories that are still represented today. In the following outline, three main theoretical streams are presented – realist, liberalist, and constructivist approaches – and how new objectives are evolved in these thoughts till today. It should be noted that all three theoretical traditions involve different security models – for example, the theory of deterrence and the theory of balance of power is also connected to realism. Hereinafter, all three will be elaborate as well as the different theories and models within certain trends.

Realist School

There are two positivist approaches in security theories encountered under realist and liberalist objectives. These are generally focusing on geopolitical power structures in comparison to the constructivist critical theories. The first scientists working on security theories are the so-called Realists focused primarily on deterrence, targeting, deployment, and impact measurement.

Realism has its roots in theories of Niccolo Machiavelli and Thomas Hobbes, who consider states as responsible actors to maintain law and order and security (Wheelan 2004). According to this approach, international institutions are not major players, states are the most important actors in the international order, and only the right balance of power can ensure international order. This political realism paradigm was originally based on three main attributes: "statism" whereby the state is the most important player in international relations, in which "survival," the maintenance of the essential needs, is the fundamental interest of every state, and finally "self-help," which refers to the behavior of states, since states are forced to guarantee their own security (Lippmann 1944). The ontology of realism is the state, especially the behavior of the great powers in which states act in their national interest and in order to preserve their own security. Therefore, they seek to increase their power in the international system. Power is therefore one of the central elements of realism.

Realists in security theories, however, take a very pessimistic view of human behavior in this regard, by assuming that states generally do not trust each other. This means that states pursue their own national interests and do not trust other states of the international system. This skepticism is rooted in the experience of the two world wars after which political realists felt that their theories were validated. This epistemological trend is built on a positivist methodology – an approach that emphasizes normative scientific measures. Accordingly, states are considered to be rational actors who always choose the option with the lowest cost but provide the greatest benefit, so they can develop their own central power structures.

Realism carries with it the logic of anarchy, which is nothing more than international conflict. Conflicts are always associated with the disruption of the international balance of power. Where the balance of power is restored, stability and peace will follow. Most realist thinkers believe that anarchy is directly linked to the proper distribution of power and at international level it produces a certain type of order. Realism holds that

> in the pursuit of foreign policy, the state must draw upon the society and economy for material resources and political support. In effect, the state's external policies depend critically on what it can extract from its domestic system. In the pursuit of foreign policy, the state finds itself giving great attention to strengthening, shaping, and developing domestic material and political resources. The sources of national power are many-political, economic, and military. " page 460 Toward a Realist Theory of State Action Author(s): Michael Mastanduno, David A. Lake and G. John Ikenberry Source: International Studies Quarterly , Dec., 1989, Vol. 33, No. 4 (Dec., 1989), pp. 457– 474

Yet, as realists believe, there is no such a structure in international relations as global government, but the lack of superior power does not exclude the possibility of an international order.

Security Dilemma

In the 1950s and 1960s of the Cold War with political tensions between the United States and the Soviet Union, government funding was available for major research projects. "In the context of the mutual nuclear threat between the United States and the Soviet Union, and the massive military capabilities of both the North Atlantic Treaty Organization (NATO) and the Warsaw Pact, it was necessary to seek ways of enhancing one's own security. Nuclear states tried to reduce the threat of their potential opponent without necessarily military measures, and to maintain the overall stability of the international system. For most of this period, however, the content of security was seen as exclusively military security against the military power of other states" (Buzan and Wæver 2007: 114). In this period, many security researches stayed initiated in the United States, particularly at RAND Corporation, which was originally a so-called US Air Force Research Center think tank. RAND has developed interdisciplinary approaches, such as the application of game theory and system analysis for a better understanding of the different nuclear strategic and security issues. In this period, many researchers from a variety of backgrounds were involved in security studies like mathematician Albert Wohlstetter, Thomas C. Schelling educated in economics, Bernard Brodie who taught political science, and even Henry A. Kissinger who was a historian. This boom in the theoretical development resulted in several new security approaches (Baldwin 1995).

There are two main objectives that shape Realist theories, offensive and defensive security approaches. Offensive realism has the similar structural logic as defensive realism; therefore, it is also called as the "little brother" of neorealism. In the offensive realist view, it is anarchy and insecurity that compel states to keep searching for opportunities to increase their power. To this end, they are also willing to risk the status quo and, if the opportunity arises, become a hegemon, for them the safest position (William 2008). This theory is mainly linked to the publication of John J. Mearsheimer entitled *The Tragedy of Power Politics* (Mearsheimer 2001).

The more popular approach among realists is Defensive realism, claiming that cooperation of states is not possible. Representatives of this theory like Robert Jervis and Charles Glaser and Stephen Walt introduce subsystem factors (such as internal political factors) in security theories (Smith and Fontanel 2008). According to them, the conquest in power structures is very complicated, so the states prefer defensive than offensive policies. Hence, defensive view can lead to a security dilemma, that was originally conceptualized by John H. Herz (1950), who set out such defensive reasoning of states in a relativist approach. In a simple way, he describes how state A would increase its military capabilities, that triggers state B to do the same, as it wouldn't feel safe and will follow suit. Accordingly, state "A" forces "B" to continue arming, which also puts state B in the direction of further militarization to increase her security. This arms race is increasingly destabilizing and can easily lead to

international conflict. According to realist literature, this process has led to World War I as a classic example. Shortly, due to the distribution of the relative abilities of security actors, there are major powers (poles) in the international system (Balogh 2013), as states have different recourses to increase their abilities. The theory includes a very interesting and controversial aspect: although both states had separately increased their own security, overall, they became more precarious, because they couldn't be sure of the other's intentions. Thus, according to the theory of the security dilemma, war is possible even if the two sides have increased their military capabilities purely for defense purposes, not with offensive intentions. This is a great representation of the states' lack of trust in a state of anarchy that dominates the international system (Booth and Wheeler 2008). Though states are very similar in that they see the same functions, their abilities are different and that is what defines the structure of the anarchic international system. Anarchy forces states to act on their own to protect their interests, and this results in an "involuntary" articulation that imposes rules on states' behavior.

Neorealism

In line with Defensive realists' theories, several objectives have been developed, such as structural realism, or with other terms neorealism. In his *Theory of International Politics (1979)*, Kenneth Waltz explores the central question: why do states with different political systems behave similarly in the international system? According to his theory, states' policies are determined by the constraints imposed by the international system. Waltz also challenges traditional notions of power by referring to cultural, economic, and political attributes. Therefore, the most important classification in Waltz's work is the distinction between "reductionist" and "systematic" theories (1879: 60).

Reductionist theories focus on unit-level variables (such as the state), but systematic theories focus on the system and prioritize system-level variables (like power sharing). As it is based on the analogy with market theory, Waltz's book focuses on the latter and explores how the international political system works. The market, according to Walt, is like international and economic operators, and those are equivalents of states. The market has certain laws. If an actor wants to remain competitive, they must follow them in order to avoid bankruptcy, which would force others to leave the market. Similarly, the state must obey the anarchic laws of the international system in order to survive. So, in order to remain competitive, the states need best practices in the system to maintain security. The system itself determinates competitive elements by rewarding certain forms of behavior, while punishing others. States learn to adapt to these rules through socialization and constant competition. The system is made up of units and their interactions; although, the system itself is determined by three factors: the order in which the components are located in the structure (anarchy or hierarchy); and the functional specification of units (states), which indicates units how and with what intensity they can perform their functions.

The Theory of Power Balance

Hans J. Morgenthau is considered the most respected theorist of modern realists today with his book *The struggle for power and peace* that was published in 1948. Morgenthau believed that the driving force behind politics has always been objective laws and human nature. The most important objective law is the idea of interest, defined by the system of concepts of power. In his theory of balance of power, Morgenthau explains thus how states balance each other's power. The balance of power is always shaped by sovereign states, following Max Weber's logic, who have a monopoly on legitimate violence. States possess weapons because of their inherent inclination conflict, so depriving them of their weapons would be futile because their willingness to stays involved in conflicts. The theory also distinguishes internal and external balance. The former refers to the internal activity of the state to increase its power and capabilities, and the latter to the establishment of alliances (Balogh 2013).

Realism recognizes the moral consequences of politics, though states' policies cannot be

governed by a universal moral code (Booth and Wheeler 2008) Accordingly, Morgenthau assumes that individuals are rational, so that their actions can be calculated within certain limits. All kinds of politics (including international politics) are defined by different actors by the effort to maintain and gain political power. He explains that security politics must be interpreted as an autonomous balance of powers that forms a coherent system. This system may include alliances or subsystems, which have their own regional power balance formation. It is held by states to maintain stability in the international system by preventing individual states or the emergence of groups of states that could endanger the security of other states. Furthermore, they control the power positions of other actors; sometimes an alliance even coordinates their activities. However, peaceful social change rarely happens and, as most realists, Morgenthau is skeptical about the role of international institutions, especially with regard to the UN. As states are constantly striving to prepare for war and the factors that upset the status quo almost always lead to international conflict, political realists always monitor the relative power of a nation and its position in the international system. This means that power must always be measured in relative terms.

The theory of threat equilibrium is a modified version of the former approach. In this theory Stephen Walt developed in *The Origin of Alliances* (1987), he claims that states control threats rather than power.

> "Walt argues that states take action to counterthreats to their security with threat level determined by four characteristics of a possible rival state: 1) aggregate power, 2) offensive power, 3) proximate power, and 4) offensive intentions. To the defensive realist operating according to balance of threat logic, the threat to state security comes first and is followed by a counterbalancing reaction. This contrasts with the offensive realist assertion that great powers are primarily assertive – not reactive – in efforts to expand their power" (Person, 2017: 45).

Although the theoretical approach of Walt was an important step in the development in Security theories, the main objective was still a positivist, narrow, military force–based approach on interstate level. With the rising dominance of liberal political paradigms, liberal security theories have gradually extended the scope of this field.

Liberalism

The events of the 1970s and 1980s brought about a significant change in the role of security studies compared to the early years of the Cold War. The oil crises emphasized the importance of interdependence and the role of international economy in security theories and justified the non-military dimensions of security and the corporate international system. This economic-political shift is raising the relevance of liberalist theories and the role of interdisciplinary studies in security theories. Epistemologically, liberalism takes a positivist approach like realism, but liberalism accepts the erosion of state autonomy if it contributes to the well-being of its citizens. The classical liberal approach in liberal political philosophy relies on Locke, Hume, Smith, and Kant (Ferenc 2001). Ontologically, instead of emphasizing the importance of the military power of a state, it emphasizes the importance of economic policies and cultural values and rejects that power politics shape international systems. There is not much skepticism about the cooperation of different actors as Realist have, but liberals also emphasize the mutual benefits of international cooperation with the participation of non-military organizations such as NGOs or commercial firms, as influencers of security politics. Thus in opposition to Realists, liberals believe that international trade makes international cooperation possible, and therefore to reach goals like peace. The United Nations and other organizations are also recognized as core actors contributing to international relations and stability. These organizations are considered as mitigating, that reduce uncertainty and have a stabilizing effect on the international system (Morgan 2007).

Collective security is one of the core concepts of liberal security theories. Collective security is a regional or collective agreement in which states guarantee their sovereignty and security. They reject international aggression and seek to resolve

their disputes by peaceful (diplomatic) means. A collective security system is supported and managed by international institutions (Roberts and Kingsbury 1993). It is based on the notion that security is indivisible and that a common response to aggression is needed.

A well-known liberal international security theory is the democratic peace theory, basically related to Michael Doyle and Bruce Russett et al. (1995). They assume that democratic states are not at war with each other. Doyle also mentions international relations' three different representations of the liberal viewpoints: the first is an interpretation of Locke, the second focuses on the importance of international trade, and the third is the Kantian concept of peace. Locke's interpretation accepts the concept of anarchy and takes into account the possibility of conflict. However, in his view, one of the most important attributes of the state is legitimacy, as it is based on representation. The second idea is international trade and the stabilizing role of capitalism, that is what generally promotes peace. The Kantian concept is based on the philosopher's idea of "eternal peace," the idea that to achieve eternal peace we need an alliance of republican governments. He also states in theory that although democratic states are not at war with one another, they are often ready to provoke non-democratic states (Doyle 1983). Michael Doyle distinguishes two approaches to the rights and freedoms of the individual: liberalism of 'laissez fair' and 'social welfare'. The first refers to the limited role of the state that advocates individual citizens' freedoms and free markets, while the 'social welfare' approach is much more in favor of expanding the role of the state for welfare purposes. Doyle distinguishes three liberal forms in international relations: distinguishes a great liberal tendency. The first is the "liberal zone of peace", which implies that liberal states generally have greater legitimacy and are thus willing to cooperate with each other, which creates the right conditions to peace.

The second trend raises the "reckless aggressiveness" of liberal states against non-liberal states. While liberal states would be less willing to risk a war against each other, non-liberal entities would fight at any time. The third approach is referred to by Doyle as "leniency and isolationism," referring to the occasional behavior of liberal states, when they are not willing to defend their allies or confront the aggressor. Examples include Nazi aggression before and during World War II and policies based on Western reconciliation.

Neoliberalism and Interdependence Theories

The above theories emphasize that a state's internal political system defines its foreign policy. This epistemic standpoint is in stark contrast to the ideas of neorealism, which are based on states being rational powers and seeking to maximize their security by acting in their own national interest, leaving out the quality of their internal political system. Robert Keohane and Joseph Nye's book *Power and Interdependence* (1977) developed a so-called complex interdependence theory, an opposing of the aforementioned approaches.

Keohane and Nye distinguished two forms of relationships: sensitivity and vulnerability. Sensitivity refers to how quickly certain political changes in one state are affected by others. Vulnerability, in turn, expresses the existence of such an alternative policy solution that addresses the negative effects of sensitivity (Azar and Moon 1984). In similar terms, liberal institutionalism emphasizes that international institutions and regimes have the power to shape international politics and international relations as well as states. International institutions are the starting point of the state activities, which follow certain standards, in particular international law rules. These institutions reinforce trust between states and facilitate agreement to sanction players who do not play by the rules. Keohane says they are also good for solving the security dilemma.

According to this theory, regimes are just as important in maintaining the stability of the international system as democracies. In Stephen Krasner's words, regimes represent "rules and decision-making procedures in a certain area of the international relations, around which the expectations of the actors can converge" (1983). Regimes control different international areas, focusing on a specific issue, such as non-proliferation. They help to reduce uncertainty, can

influence states' actions on a particular issue, and are predictable and they can also make the actions and intentions of other states transparent (Dannreuther 2014).

Another theory of global governance is linked to James Rosenau's name (1992). He claims that even if global government is not possible to establish, global governance itself is feasible with international institutions, regimes, NGOs, states, and so on. A global network of these actors can counteract the lack of global power. Shortly, the institutions of a world-wide network of regimes and other actors determine the rules needed to govern the spheres of international relations and provide a sense of stability (Rosenau et al. 1992).

Integration theories overlap with certain liberal institutionalist theories. According to integration theories, security can best be guaranteed by the integration of different policy areas and actors. Integration institutions (such as European Community) give impetus to further development and the integration process itself as well as playing a central role in integration theories such as neofunctionalism. Ernst B. Haas and Mitrany are the founding thinkers of neofunctionalism who outlined the global integration of different political functions primarily in the technological, economic, and social spheres. According to the theory of neofunctionalism, various interest groups in a particular political or functional area have a cross-border dimension where links are established to further the integration process. If one functional area has been integrated internationally, this integration has a so-called spill-over effect on other areas, and so in some areas leads to gradual unification (Rosamond 2005). In this way, the theory is closely linked to the European Union, as the history and development of European integration is often examined through the lens of neofunctionalism (Haas 1975).

Liberal hegemony is a liberal version of hegemonic stability theory. According to this concept, a liberal hegemon serves the interests of other states in the international system by promoting liberal values. Like realist hegemony theories, liberal hegemons provide public goods such as security, order, etc., but the most important common good it has to offer is the spread of liberal values (Collins 2016).

Human Security

During the Cold War, national security strategies were primarily territorial and against threats from the outside with a government and an army considered as responsible for guaranteeing human safety. In contrast, over the past two decades, new frameworks are developed to adjust the scope of security objectives as more and more new security challenges were difficult to conceptualize within the earlier prominent tools which become inadequate to deal with these changes. One of these approaches is the so-called human security theory, which proposes a people-centered approach instead of state-centered security concepts, with the emphasis on protecting individuals. In his new theory, the scope of the investigation is extended by new elements in terms of actors and tools. The concept of human security focuses not only on defense, but also on prevention (rather than on the generally defensive nature of military security based on arms race and strategic alliances). The first milestone in the development of the theory of human security is the Human Development Report (UNDP 1994) that first drew attention to security *and* development due to a large number of conflicts within states which were taking place in the form of civil wars, not between states. This approach is in stark contrast to the ideas of realism, which considers states as the basic unit of security (reference object). According to the theory of human security, the individual must be the reference object and every factor that endangers an individual, either physically or psychologically, should be understood as a security threat. This is especially true if we take into account that sometimes the state poses a threat to its own citizens. By explaining such situations, this human-centered approach introduces new difficulties for positivists, because this theory calls into question the state-centered views of realism and is therefore bound to constructivism and critical security studies (Kerr 2009).

In theoretical terms, two academic groups made such broadening efforts. In one new approach, the novelty was provided by the expansion of security policy actors. According to this group, the key to understand new types of conflicts, such as terrorist attacks, is not about loyalty to states or conflicts between them, but a clearer understanding of the identity circumstances behind "sub-state violence" ("blood and belonging"). It should be noted, however, that this group is probably rightly criticized for defining the various forms of irregular and asymmetric wars and terrorism today as a new type of conflict. According to this criticism of the non-state protagonists, these events should not deny the Clausewitz conceptual framework, namely that war is the pursuit of politics by other means. Accordingly, there is always political intent behind civil wars, ethnic and religious conflicts or terrorist acts, but the actions are not security issues, they are simple law enforcement and criminal law issues.

Other theorists argue that challenges, such as cross-border organized crime, necessitate greater involvement of non-military threats in security studies. This has led to the concept of human security today. It is now more or less generally accepted that beside state actors in international politics other actors are also playing an increasingly important role in the international system. Non-state actors such as multinationals, terrorist organizations, environmental organizations, international foundations, civil and church organizations, or non-state nations, such as Kurds, can also create and develop their own private and non-governmental security policies. Multinational companies, especially since the 1990s, are increasingly relying on private military and security companies to protect their interests. Our globalizing world is now accompanied by global terrorism. Democratic societies are increasingly forced to take into account these international actors like reports of Amnesty International. These power relationships would result in less conflict and greater stability at national, regional, and global levels. Thus, on the one hand, the focus shifts from the state to the individual, but on the other hand, the scope is different: the classic concept of security that states protect against external aggression is challenges, and in human security this concept is complemented by wider threats, such as pollution or epidemics. Instead of the state's exclusive role (decision-making and monopoly on violence), "non-state actors play a key role in providing security" and as a result the fundamental concept of security is reworded and expanded (Newman 2010: 78).

So instead of territorial security, the focus should be on the security of the individual, and on the concept of (sustainable) development instead of weaponry. Thus, the concept of individual security has shifted toward meeting needs, and as a result, human security has been linked to economic development. However, the report emphasizes that human security is not equivalent to human development. Development is a broader concept, and its main goal is to provide people with more choices in all areas of life. In contrast, the concept of human security is a broad one, seeking at enlarging individuals' choices by "assuring priority freedoms so that 'people can exercise choices safely and freely' (HDR 1994, page 23) and can be confident that the opportunities they have are protected" (Gomez et al. 2013). Consequently, there is a kind of interdependence between the two areas that the failure of one area is likely to have a negative impact on the functioning of the other and is likely to accelerate its decline. Indeed, over the past decades, putting the theory into practice has led to the emergence of two schools, one of which is attributed to each of the major threats, both taking (the lack of) freedom as a core starting point.

Hence, in the economic sector, it is much more difficult to identify the real threat than in the military and political sectors. In the social sector, it is primarily nations, ethnicities, or religions that may be threatened. However, since community identities are constantly evolving in response to external and internal influences, it is often extremely difficult to draw clear boundaries and distinguish between a life threat and a lesser threat. If our identity is more conservative, we are also more inclined to regard some of these natural changes as a threat to our identity, even when others do not experience the changes. For

example, the ability to maintain language, behavioral habits, or ethnic purity is generally regarded as survival, and the loss of this ability is a threat to life, although the latter may have a different meaning (Kaldor et al. 2007).

As far as the environmental sector is concerned, there are quite obvious cases at both macro and micro level that can be secured. The survival of a species or habitat, in more general terms, the biological heritage of mankind, a change in the usual climatic environment, and the maintenance of an advanced level of human civilization can be interpreted as security issues. However, like the economic sector, we find a set of problems in the environmental sector that are much more difficult, though not impossible, to formulate as a threat to life. As it will be illustrated, this widened conceptualization become very popular among constructivists, and critical theorist emphasize that it should be situationally reconsidered whether a given question is really a security issue or something else. In summary, the threat to security – that is, the factors that negatively impact security – is seized with the concepts of threat, potential threat, and risk and national security strategies (Brauch 2005).

Constructivist Approach and the Critical Schools

New security challenges after the Cold War gave new incentives to think in security theories. The United States and Europe followed a different path in these developments after 1980s and 1990s. European security studies are much more inclined toward international security issues, more critical, and in contrast with positivists; it is established on the constructivist (Neo)Marxist approach. North American scientists use a more traditional theoretical perspective and US experts have remained more closely involved in political decision-making. In Europe, there are three main schools registered within the framework of Critical Security Studies: the Paris School, the Whales School, and the Copenhagen School. Based on these reflective approaches, recent Critical Security Studies inspired many academics and experts who left conventional positivist security frameworks (Realism and Liberalism) to gain a better understanding of contemporary (in)security issues. Also, many recent theories elaborated Security theories with engaging other disciplines and progressive radical theories, such as critical feminism or environmental theories, as well as Neo-Colonialism or Race theories. Before the different schools would be elaborated, it is important to highlight the main epistemic difference between the previous Security theories and the Critical.

As the core epistemological foundation of Critical security theories, (Neo) Marxism deals with certain aspects of material reality, though it tends to question the status quo and power order, both at the sub-state level and internationally, which already entails a kind of criticism. The original theory is linked to the work of Georg Wilhelm, Friedrich Hegel, and Karl Marx. Marx, in his 1867 book, *Capital,* he expressed his views on privileged social classes with appropriate certain resources, such as capital. Marx argues that the capitalist class benefits from withholding wages because they keep to themselves the difference between the value of the work produced and the wages actually paid. According to Marx, the means of production are in the hands of the capitalist class, so it is a privileged position that creates tension between capitalists and the working class. All social relations and society as a whole, with all its subsystems ("superstructures"), are based on the economy ("basic"). Neo-Marxism is associated with Antonio Gramsci, who emphasized in his works that the state and the ruling class are in a hegemonic position within society that can only be sustained through the cultural hegemony of capitalism (Fontana 2008). Robert Cox is one of the most influential Marxists in international relations. Cox used Gramsci's theory to the international system and explained that the international capitalist class maintains its international hegemony through the culture of capitalism. So, Marxism focuses on transnationally connected and organized departments and class interests in place of military power of nation states (Cox 1987). Another well-known neo-Marxist interpretation is Immanuel

Wallerstein's "world system theory", which Wallerstein based on his early work. In his view, capitalism is a world system made up of three types of entities: an economically advanced center (core) that dominates the entities belonging to the semi-periphery and the periphery.

The latter mainly provides cheap raw materials and also cheap labor for core areas and as a market services the core technology of modern products.

The core area retains its economic and political priority through its economic relations with the periphery and the periphery. The semi-periphery is a mixed category of entities that strive to catch the core while the states of the periphery try to join those at the semi-periphery. Neo-Marxist thinking is very similar to Constructivism considering the ideology on the monopoly of power or system of norms that is interpreted by the result of its core function, namely to maintain the power of certain classes and through generations of hegemony and social status reproduction (1974).

Constructivism arose from the transposition of critical theories into political science, sociology, and philosophy in international relations. In these disciplines, Constructivism is closely linked to the Frankfurt School and its renowned scholars such as Theodor Adorno. According to Michael Barnett, in order to understand how different ideas, ideologies, and power structures are played out in different contexts, all types of political power acts and statements must be broken down in order to better understand reality. This view in international relations had a peak between the 1970s and 1990s, and was associated with, among many others, Peter J. Katzenstein and Alexander Wendt. In their view, the national security environment of a state and security politics is primarily determined by cultural and institutional aspects, and non-material elements such as collective values, culture, and social identities. They thus determine the identity of the state, which in turn is decisive in shaping state policy. Accordingly, "international reality is socially constructed by cognitive structures which give meaning to the material world" (Adler 1997: 250).

According to a constructivist interpretation of Wendt, international politics is thus a construct that reflects a certain type of shared knowledge and a set of norms about reality. These norms are the result of the interaction of actors in the international system. Identities are built through interaction, and these determine the interests of the states – so the national interest is a construct. This however influences the actions of the state and material reality too. The central role of ideals and norms is what is essential for the international system to understand its structure and the behavior of states (Wendt 1999).

The Welsh School

The Welsh School (or Aberystwyth School), also known as emancipatory realism, is differentiated from the other critical schools by exclusively requiring Critical Security Studies (CSS) as the theory of studying security issues (Peoples and Williams 2014: 14). By combining Radical International Relations Theory with Critical Theories – based on the Frankfurt School and Gramscian thinking – academics Ken Booth and Richard Wyn Jones distinguished their approach from other critical approaches below (Peoples and Williams 2014).

They do not only reject the realist scope that considers states as the key security referent (defective, irrational, and too distinct) (Booth 1991: 320), but also reject the Copenhagen School in their supposition that only the threats of security are socially constructed, while the security objects are stable (Buzan et al. 1998). From the CSS viewpoint, both threat and object are social constructs (Mutimer 2016: 95).

The CSS believe that the inter-subjectivity significantly determines the variety of perspectives in security concepts that further construct it as a contested concept (Collins 2010: 3). According to these authors, security is what we define as such. This contested inter-subjective definition of security also challenges the Human Security approach in how it defines security (Lum et al. 2018). In the core, security is based on the set notion of the protection of all essential parts of human lives from any decisive and persistent dangers (Balogh 2013). Emancipation of this inter-subjective security is the only way to achieve the real security and the freedom of anyone or any group from any threats that restrict their free will

to choose what to do (political repression, deprived education, poverty, etc.) (Booth 1991: 319).

The Paris School

Another important critical school, studying processes of (in)security and (in)securitization, has been established by the so-called Paris School scholars. "PARIS is an acronym for Political Anthropological Research for International Sociology" (Bigo and McCluskey 2018: 116). The most prominent member of the Paris school is the French sociologist Didier Bigo, who has been joined by a number of likeminded scholars such as Laurent Bonelli, Ayse Ceyhan, John Crowley, Anastassia Tsoukala, all of whom place great emphasis on the utility of Foucault for the study of security (Bigo 2005). Bigo highlights "how different bodies of knowledge are labeling security, examining the tensions and controversies between and within practitioners and disciplinary fields in these labeling practices. It analyses different intellectual ways to study the relationship between the "security" label and the boundaries of "security" practices alternatively labelled by others' freedom, mobility, violence, or privacy" (Bigo and McCluskey 2018: 116).

This school treats security also as a social construction, opposed to an objective reality. Different and new to their analysis is, however, what they understand by security. Whilst, for example, the Copenhagen school of security studies claims that security is what is done with it (or better, security is what it does by speech act) (Buzan et al. 1998), Bigo turns this argument on its head and argues that '*what is done with it [how security is practiced] determines security'* (Bigo 2001). To understand what Bigo means by this, it is necessary to dig a little deeper. All of Bigo's (and by extension the Paris school's) works are informed by the same key assumption, namely that there is a merger of – what he calls – 'internal' and 'external' security into a 'field of security', whereby the border between the two ceases to exist. The border between 'internal' and 'external' here is tantamount to the borders of sovereign nation states. This school emphasizes the study of borders and boundaries, especially where discussions of the 'field of security' and the security 'ban-opticon' are concerned (Bigo 2008). This theoretical school studies the functional and de-localized dimensions of state borders as they are practiced and enforced within and beyond the territorial jurisdictions of states.

The Copenhagen School

The Copenhagen School, also known by the introduction of the concept 'Securitization', is the most known Critical approach in Security theories funded by Buzan et al. (2003). The Copenhagen School has represented "a move away from traditional security studies and drew more attention on non-military issues and non-state actors and places" (Lin 2011: 17) in order to develop a constructivist discussion of 'security networks' or 'security apparatus', emphasizing the ability of political authorities to determine what can become a security issue or a threat.

Buzan and his colleagues reflect at traditional regional security complex (RSC) theory, "with its military-political focus, and its firm regionalizing logic" (Buzan 2003: 140), and explain how this RSC is limited to several more or less disconnected systems that exist simultaneously, like international subsystems (Buzan et al. 1998: 6). With the extension of this traditional framework, these critical scholars started to invite others to "elaborate changes in the nature of the security agenda, examining the rise of economic and environmental security, with their new types of threat and new referent objects, and the decline in salience of military-political security issues amongst the great powers" (Buzan 2003: 140). These theorists encourage reflection on the political and ethical implications of the traditional assumption that security means considering the preservation of state sovereignty and territorial integrity.

In their multi sectoral approach to security Buzan, Wæver and De Wilde claimed that security should be upheld split for more detailed analysis. Five security sectors have been proposed – political, economic, military, social, and environmental sectors and elaborated how economic threats become more diverse and therefore the security object would be more complicated.

According to the authors, states in general do not regard economic threats as existential threat (but the 2008 global economic crisis has shown the opposite), and military sector can obviously bring military threats to the state but the Social Dimension of security is also challenging as there is a broad collective identity of certain groups within society with different expectations. In addition, the growing environmental sector covers the security situation of the environment at various levels today, so contrary to (neo)realism, the Copenhagen School questions the uniform nature of the state and the normative definition of threat. Their model contains four conceptual elements: "reference object", "security actor", "existential threat", and "extraordinary measures". According to the Copenhagen school, security actor is the person who turns the matter into a security issue – this actor is mostly the state. And it does so *by declaring something of an existential threat to justify extreme political action*. The most important consequence here is that the whole process is unlikely to be true, but in the best interests of the security agent, which is usually state or political power. This is the process that is extensively used now as 'Securitization' theory.

Subjectivity and the *Securitization* Process

As it was already recognized in the 1960s – security can be approached objectively (real threat) and subjectively (threat perception), and it is by no means certain that these two approaches always coincide. Moreover, a more objective approach only seems attractive at first glance. Indeed, no security theory has created an objective measure of security that can be used to determine with certainty whether a question is "really" a threat or not. Unless, of course, such cases occur most frequently in the military and political spheres when the threat is quite obvious: for example, when enemy tanks cross the border of a country.

Another major difficulty in establishing an objective standard is that security is always about assumptions about the future, about current facts, about what happens if we do not take "security steps" (these threats), and what happens when we do (how do security measures work). With the widening of Security theories there was an increasing versatile approach to security in the 1990s that was strongly correlated with (Neo)constructivist concepts.

After the oil crises of the 1970s in the UN reports of environmental and non-military sectors (such as the Bruntland Commission Report in 1980 or the Palme Committee in 1982) have blurred the boundary between security in military and non-military sectors and introduced a global approach to international security issues. This process is largely interlinked with the concepts of Buzan et al. (1998), on securitization emphasizing the ability of political authorities to determine what can become a security issue or a threat. The theory highlights the somewhat debilitating process that protects against a particular threat or matter question, and which process reflects the interests of the "security actor".

This approach elaborated the diversity of security communities, a concept developed in 1957 by Karl Deutsch et al. that includes both liberal and constructivist elements. Deutsch says that members of the community settle their disputes peacefully and share the same expectations of a peaceful social change. It differentiates between pluralist security communities like the EU and merged security communities like the United States. Adler and Barnett, who put it in a constructivist perspective, argue that security communities have been based on shared values and members with similar identities (1998). Another version of this complex theory is associated with the classic book *Regions and Powers* (Buzan et al. 2003). In this theoretical manifesto, the authors define regions as essential building blocks of international security because, according to the authors, the same members of the regions share a common security concept and are interdependent. Therefore, in case of security issues, states in a region cannot be completely separated. According to Barry Buzan and colleagues, we can talk about the following levels of analysis: international systems (such as today's global international system); international subsystems (regional systems such as ASEAN); units (such as states); actors within the unit (different organizations); and individuals

(Buzan et al. 2006). The securitization process is therefore extremely complex.

Hedley Bull, linked to the English School of International Relations, created the concept of state society (Little 2000). This is a mixed theory which consists realism, and it carries the hallmarks of liberalism, but it also contains critical elements, that justifies its reference here among critical approaches. Bull argues, despite its material reality, the common norms and underlying values that shape international politics. States participate in the work of international organizations and institutions; they influence each other and share certain norms and values. These interactions are manifested through a process of socialization that leads to the society of the states in the international system. The English school accepts the concept of anarchy, but it also emphasise the role of international organizations as well as the role of international laws (Jones 1981). However, anarchy can be mitigated by a sense of community (society) between states, which results in states that are able to accept certain common norms and values.

This securitization theory thus emphasizes that the outcome is shaped by a political process and not necessarily a scientific investigation of the threat. It encompasses the long-term experiences of the collective memory of a given society (think of the Armenian and Jewish Holocaust), the aspirations of opinion-forming strata – intellectuals, economic and political elites (for example, inciting the nationalism of Yugoslav nations in the 1980s and 1990s), as well as the state's geostrategic interests. The problem of defining *security* and *securing a given reference object* is closely linked to the question of the level of analysis. Security theories and securitization can be interpreted on several levels depending on the particular actor what is its purpose.

Criticism

In the ontological sense, the critical tendencies question the traditionally material ontology of theoretical schools such as realism or liberalism. Realism and liberalism accept the concept of objective reality. Realists and liberal thinkers are concerned with details of the material aspects of reality that they can be measured more or less objectively and numerically, e.g., economic variables, military power, territory, population, etc. However, critical approaches deal with its non-material dimension, such as norms, principles, ideas, ideologies, identities, ways of thinking, and cognitive processes. It also means that Critical security thinking does not believe in objective reality, but instead examines the subjective side of understanding reality. "This issue driven widening (of the critical schools and human security theories) eventually triggered its own reaction creating a plea for confinement of security studies to issues centered around the threat or use of force" (Buzan 1997: 6).

"A key argument was that progressive widening endangered the intellectual coherence of security, putting so much into it that it's essential meaning become void. This argument perhaps masked a generally unspoken political concern that allowing non-military issues to achieve security status would have undesirable and counterproductive effects on the entire fabric of social and international relations" (Buzan et al. 1998: 2). According to traditionalists, the concept of security should continue to focus on traditional issues, such as the use or threat of military force while critics believed that the concept of security should be expanded to new non-military nature areas such as the environment, society, and the economy (Collins 2016).

It was also claimed that these critical approaches are Eurocentric; realists accused critical theorists with "intellectual incoherence" and some have criticized the absence of gender roles. In a sense, with the expansions of non-traditionalists after the end of the Cold War together with traditional (military) security interpretations prevailed and has been later extended by new security approaches such as queer theory in IR.

Queer Theory

Theories of feminist security studies and feminist international relations are closely related to constructivism and Marxism. Marxist Feminism, for example, highlights the Marxist roots of feminism. Feminist security thinking draws attention to the current neglect of traditional approaches

research areas such as gender issues, women's rights, vulnerable groups (minorities), children, and the environment. Of course, most of these issues are of increasing importance in times of international conflict. Feminism contributes great importance to security studies, in particular how international conflicts and civil wars affect voulnerable groups considering gender related questions. Warfare is usually tied to men and is traditionally considered a men's business. However, it is women and children who are most vulnerable to conflict and their best interests are never represented in the war when making political decisions. Feminism also seeks to raise awareness on neglecting environmental issues – in general and during armed conflicts too. This is an aspect that traditional approaches completely ignore. In addition, Queer studies represent the ways in which sexualities and gender affect international security, like how some groups become disciplined by traditional sites of power; like how queer identities are subjected to domestic and foreign policy in heteronormative contexts. Ontologically, these theories aim to highlight the position of various marginal groups from a constructivist security approach and show how liminality and visibility is played out in international power relations. At last, epistemologically, this objective covers alternative methodologies to security theories, in particular, to understand intergroup relations behind existing formal bureaucratic entities.

Conclusion

This review aims to provide a brief insight into security theories. In addition to the aforementioned schools, there are many more security theories, but due to the limited framework these could not be discussed here. The richness of every scientific discipline is best demonstrated by its heterogeneity that engenders intellectual debates that further extend our understanding of reality. This also means, of course, that neither theory is "better" or "worse" than the other. These are just theories that have different ontological and epistemological beliefs. We could say that every theory has its own strengths and its weaknesses, and all situations should be handled with the right approach. This heterogeneity also demonstrates the complexity and diversity of societies and demonstrates the multitude of disciplines that offer an understanding of international security issues. Thus, the analyst or scientist must choose carefully the right theory to understand a case in a specific context.

Cross-References

- ▶ Risk Analysis: National and International Standards
- ▶ Security: Concepts and Definitions
- ▶ Security Management
- ▶ Security: Private

References

Adler, E. (1997). Seizing the middle ground: Constructivism in world politics. *European Journal of International Relations, 3*(3), 319–363.

Azar, E., & Moon, C. I. (1984). Third world national security: Toward a new conceptual framework. *International Interactions, 11*(2), 103–135.

Baldwin, D. A. (1995). Security studies and the end of the Cold War.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies, 23*(1), 5–26.

Balogh, I. (2013). Biztonságelméletek. *Nemzet és Biztonság, 3*(4), 36–56.

Bigo, D. (2001). *A fresh look at conflicts. The New International Relations. Theory and Practice. M.-C. Smouts* (pp. 171–198). London: Hurst & Company.

Bigo, D. (2005). The globalization of in (security). *Cultures Conflits, 58*(2), 3–3.

Bigo, D. (2008). Globalized (in) security: The field and the ban-opticon. In *Terror, insecurity and liberty* (pp. 20–58). London: Routledge.

Bigo, D., & McCluskey, E. (2018). What is a PARIS approach to (in) securitization? Political anthropological research for. *The Oxford Handbook of International Security*, 116.

Booth, K. (1991). Security and emancipation. *Review of International Studies, 17*(4), 313–326.

Booth, K., & Wheeler, N. J. (2008). *The security dilemma: Fear, cooperation and Trust in World Politics*. New York: Palgrave Macmillan.

Brauch, H. G. (2005). *Environment and human security: Towards freedom from hazard impacts*. UNU-EHS.

Buzan, B. (1997). Rethinking security after the cold war. *Cooperation and Conflict, 32*(1), 5–28.

Buzan, B. (2003). Regional security complex theory in the post-cold war world. In *Theories of new regionalism* (pp. 140–159). London: Palgrave Macmillan.

Buzan, B., & Wæver, O. (2007). After the return to theory: The past, present and future of security studies. In A. Collins (Ed.), *Security studies* (pp. 386–387). Oxford: Oxford University Press.

Buzan, B., Buzan, B. G., W'ver, O., Waever, O., & Buzan, O. W. B. (2003). *Regions and powers: The structure of international security* (No. 91). Cambridge: Cambridge University Press.

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Collins, A. (Ed.). (2016). *Contemporary security studies*. Oxford: Oxford University Press.

Colins, S., & Cohen, E. (Eds.). (2007). *Strategy in the contemporary world* (2nd ed.). Oxford: Oxford University Press.

Cox, R. W. (1987). *Production, power and world order: Social forces in the making of history*. New York: Columbia University Press.

Dannreuther, R. (2014). *International security: The contemporary agenda*. Wiley.

Doyle, M. (1983). Liberal legacies, and foreign affairs, Part 2 philosophy & public affairs, Vol. 12, No. 4 (Autumn, 1983), pp. 323–353.

Ferenc, G. (2001). *Biztonságpolitika*. Budapest: SVKH.

Fontana, B. (2008). Hegemony and power in Gramsci. In *Hegemony* (pp. 92–118). Routledge.

Gazdag, F. (2011). *Biztonsági tanulmányok–biztonságpolitika*. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem.

Gomez, O. A., Gasper, D., & Mine, Y. (2013). Good practices in addressing human security through national human development reports. Available at SSRN 2552757.

Haas, E. B. (1975). *The obsolescence of regional integration theory* (Vol. 25). Berkeley: Institute of International Studies, University of California.

Herz, J. H. (1950). Idealist internationalism and the security dilemma. *World Politics, 2*(2), 157–180.

Jones, R. E. (1981). The English school of international relations: A case for closure. *Review of International Studies, 7*(1), 1–13.

Kaldor, M., Martin, M., & Selchow, S. (2007). Human security: A new strategic narrative for Europe. *International Affairs, 83*(2), 273–288.

Kerr, P. (2009). Human security and diplomacy. In *The Routledge Handbook of Security Studies* (pp. 131–142). Routledge.

Lin, L. (2011). State-centric security and its limitations: The case of transnational organized crime. Research Institute for European and American Studies (RIEAS).

Little, R. (2000). The English School's contribution to the study of international relations. *European Journal of International Relations, 6*(3), 395–422.

Lippmann, W. (1944). *US war aims*. Da Capo Press.

Lum, C., Cave, B., & Nichols, J. (2018). Are federal security efforts evidence-based?. *Security Journal, 31*(1), 139–162.

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. New York: WW Norton & Company.

Morgan, P. (2007). Security in international politics: Traditional approaches. In *Contemporary Security Studies* (pp. 11–34). New York: Oxford University Press.

Morgenthau, H., & Nations, P. A. (1948). *The struggle for power and peace*. Nova York: Alfred Kopf.

Mutimer, D. (2016). Critical security studies. In M. D. Cavelty & T. Balzacq (Eds.), *Routledge handbook of security studies*. Routledge.

Newman, E. (2010). Critical human security studies. *Review of International Studies, 36*(1), 77–94.

Peoples, C., & Vaughan-Williams, N. (2014). *Critical security studies: An introduction*. Routledge.

Ritch, J. (2001). The future of nuclear energy in an era of environmental crisis and terrorist challenge (No. IAEA-SM–367/CD).

Roberts, A., & Kingsbury, B. (1993). Introduction: The UN's roles in international society since 1945. United Nations, Divided World: The UN in International Relations, Clarendon Press, Oxford, 1–63.

Rosamond, B. (2005). The uniting of Europe and the foundation of EU studies: Revisiting the neofunctionalism of Ernst B. Haas. *Journal of European Public Policy, 12*(2), 237–254.

Rosenau, J. N., Czempiel, E. O., & Smith, S. (Eds.). (1992). *Governance without government: Order and change in world politics* (Vol. 20). Cambridge University Press.

Russett, B., Layne, C., Spiro, D. E., & Doyle, M. W. (1995). The democratic peace. *International Security, 19*(4), 164–184.

Smith, R., & Fontanel, J. (2008). International security, defence economics and the powers of nations. *War, Peace and Security, 6*, 37À52.

United Nations Development Program. (1994). Human Development Report 1994 Forrás. http://hdr.undp.org/en/reports/global/hdr1994/

Wendt, A. (1999). *Social theory of international politics*. Cambridge: Cambridge University Press.

Wheelan, J. (2004). *Jefferson's war: America's first war on terror 1801–1805*. Public Affairs.

Williams, P. D. (Ed.). (2012). *Security studies: An introduction*. Routledge.

Security Guards: Academic and Training Programs

Brian P. Kelly[1] and Paul J. Schmick[2]
[1]Security Systems and Law Enforcement Technology, Farmingdale State College, Farmingdale, NY, USA
[2]Alliance Security, New York, NY, USA

Keywords
Human security · Guards · Asset protection · Training · Academics · Programming · ASIS International

Definition

Security guards include people employed primarily to perform one or more of the following duties: protection of persons and/or property from harm, theft, and/or unlawful activity; deterrence, observation, detection, and/or reporting unlawful or unauthorized activity; street patrol service; and response to, but not installation or service of, a security system alarm (New York State Department of Licensing 2018).

Introduction

In 2017, 810,000 security guards were employed by industry in the United States with revenue produced topping 25.5 billion (Statista 2018). Variables, such as ample spending and the challenge to reduce liability, justify the importance of training and, where academia can assist, in cultivating personnel who are charged with non-law enforcement responsibilities but who serve as a deterrent and protective layer between theft and physical harm of the public. Program costs will affect the willingness of contract security guard firms to absorb training and development for their staff based on their return on investment.

Academic and training programs have evolved over the years to meet a set of general, minimum standards required by the security industry (e.g., age, residency, high school diploma/GED). Security academic and training programs allow students to reduce risk and liability of "excessive" acts of the profession, as well as provide avenues for students to learn new security methodologies and update their existing knowledge and skills in the field (MBAskool 2018). It should be noted, however, that there is no uniform or national set of standards; instead, individual states determine standards required for certification and employment of security guard forces.

The purpose of this entry is to provide students and professionals with information about types of academic and training programs available for security guards within the United States. The elements that comprise and encompass training programs within regions of our nation that differ in required mandates are reviewed. Additionally, national organizations and academic institutions which possess the resources and capabilities to disseminate course work within this area of subject matter, in traditional and online platforms, are provided.

Security Concerns

Various state-level legislative and regulatory issues and challenges for contract security companies are monitored by the National Association of Security Companies (Amitay 2013). Stakeholders in different regions of industry have increased their financial budgets to cover the use and hiring of security personnel as a means of providing effective protection of their assets and personnel. As the number and types of threats to safety and security have evolved over the past decade, the need to measure and gauge the level of training, knowledge, and capabilities of security guards must increase proportionally. For example, the 2013 *Washington Navy Yard* mass shooting attack raised important issues and challenges related to the adequacy of federal facility security, access control, and personnel background screening. Unfortunately, this active shooter attack was but one of several other recent shootings at federally protected facilities.

Federal agencies and their contract security partners who protect assets and personnel at those facilities must work together to address and develop new efficient and effective strategies to reduce the current risks and threats (Amitay 2013; see Critical infrastructure: Government facilities sector in this encyclopedia). The Department of Homeland Security's (DHS) Federal Protective Service (FPS) is the primary agency responsible for providing law enforcement and related security services for the approximately 9,600 federal facilities under the control and custody of the General Services Administration (GSA). FPS has about 1,200 full-time employees and about 13,500 contract "protective security officers" (PSO's) deployed at thousands of federal facilities (generally Federal Security Level III and IV facilities) of GSA's 9,600 facilities (Duncan 2013). The remainder of the federal buildings and structures are protected by three dozen other federal executive branch agencies.

Not including the military services, there are approximately 35,000 private security officers working for various federal agencies (Amitay 2013). Contract security organizations [see Contract: Security in this encyclopedia] are responsible for the employment, delivery, and training of this capable human resource. At minimum, they must be able to select and sustain properly a higher level of security guard to work within critical infrastructures, as well as other properties deemed hard and soft targets. Potential contract security employees must be taught the appropriate knowledge, skills, and abilities to work competently in this capacity. However, not all of the academic and training programs for security guards are equipped by reputable service providers, up to par based on perceptions of global security service providers, or available in every state.

Assessing Needs: Limiting Liability and Increasing Accountability

It still remains a challenge to find credible information on the number of people working in the contract security industry in the United States (Perry 2016). Nonetheless, it may best advantageous to perform an analysis or reference reported case studies to determine how a synergy of training, education, and technology investment opportunities may offer ideal performance of security guards. Most importantly, applicants should evaluate programs to determine which may offer successful future outcomes during times of escalation, as well as limit employee and employer exposure to liability and lawsuit and, in most extreme circumstances, prevent incarceration of security guard personnel.

In one case, Smith (2018) analyzed conflict escalation resulting in the November 29, 2017, event resulting in an altercation between three contract security guards and residents at Pamoja Men's Homeless Shelter in Bedford Stuyvesant, New York. Captured through surveillance cameras, security guard personnel failed to execute restraint and met resistance with offensive tactics resulting in a guard's termination, a supervisor's demotion, and a civil lawsuit by residents against the City of New York. In addition, the City of New York sued the contract security firm. Litigation is pending and is tied to reports over a 36-month period in which two large New York security firms were accused repeatedly of enabling, and in some cases aggravating, violence inside city-funded shelters.

A second case study can be evaluated through the lens of excessive force in a May 2018 incident in which a security guard was charged with assaulting a teenager accused of shoplifting $850 worth of merchandise from the retailer – Century 21 Department Store in New York. Gstalter (2018) cited witnesses' accounts of security guard staff "choking" the petty thief to restrain her until law enforcement arrived. One security guard was arrested for assault. While the heist was labeled a petit larceny and possession of stolen goods, litigation pending will most likely result in damages awarded due to excessive force by the security staff who are legally responsible under New York State law to only "observe and report" unless defensive measures are appropriate to defend oneself.

A most extreme case involving confrontation between the security guard staff and a hospital

patient resulting in death offers an extreme case review of the questions of risk, liability, excessive force, and, ultimately, training. Alexander (2018) cited the September 29, 2015, MedStar Washington Hospital Center case in which security staff engaged a patient behaving aggressively that resulted in that patient's death. While reports have the patient suffering from a preexisting spinal condition, DC prosecutors alleged that security guard personnel used excessive force to restrain the patient, violently tackling him to the ground and ultimately causing a fatal neck injury. Although the intent of the security guard personnel was to restrain the patient, prosecutors charged two of them with involuntary manslaughter in the death of the 74-year-old patient. As a result, MedStar Washington Hospital spokeswoman called the patient's death a "devastating and transformational moment" for the hospital, stating it will lead to changes involving the hiring and training of public safety personnel at the hospital. Such action to limit future risk and liability has also resulted in changes in the training of caregivers and security officers and the establishment of a new team to respond to "high risk."

Academic and Training Programs

Security guard performance and liability are at the crossroads for the profession in review of performance concerns in modern times (Amitay 2013). Ultimately, an analysis of return on investment should be explored and bolstered for employment organizations which seek to reduce both liability and risk of ill-prepared personnel to meet the demands of the profession and expectations of the public and industry. Nonetheless, critical facility security may not be as simple as posting additional guards. As a practical matter, the effectiveness of guards in countering a terrorist attack depends on the specific types of threats the guards may face, the training they receive, their organization, the conditions of their employment, and background checks (Parfomak and Library of Congress 2004; see Personnel Security: Hiring, Personnel Security: Recruitment, and Personnel Security: Selection in this encyclopedia).

Academia in recent years has studied facets of the expanding market, as well as limiting liability of physical confrontation between security guard personnel and the public. As listed in Table 1, the existence of undergraduate programs currently accredited in the United States whose focal points encompass private security also maintains standards that incorporate security concepts such as physical, information, personnel, as well as other security-related areas. In general, these US-based colleges strive to provide their students with the type of knowledge needed for future positions in security, both in the public and private sectors. In particular, most of the undergraduate programs' curriculum are multifaceted and diverse, as industry standards for the field of security seem to be changing often in post 9/11 times.

In contrast, as seen in Table 2, graduate programs help students to focus on a specialized areas to improve their expertise in the field, gain skills in management, and/or blend

Security Guards: Academic and Training Programs, Table 1 Security undergraduate programs in the United States

College	Undergraduate degrees offered
Bloomsburg University of Penn	BS in Digital Forensics
California University of Penn	BS in Homeland Security
Eastern Kentucky University	AS (Homeland Security or Security Management concentration); BS in Homeland Security
George Washington University	BS in Cybersecurity; BPS in Police and Security Studies
Georgetown University, Walsh School of Foreign Service	BSFS/MA Security Studies
John Jay College	BS in Security Management
Mercy College	BS in Corporate and Homeland Security
Missouri State University	BA in Global Studies
SUNY Farmingdale	BS in Security Systems
University of Maryland	BS in Computer Networks and Cybersecurity
Virginia Commonwealth University	BA in Homeland Security and Emergency Preparedness

Security Guards: Academic and Training Programs, Table 2 Security graduate programs in the United States

College	Graduate degrees offered
Anna Maria College	MA in Security Management
Auburn University at Montgomery	MS in Justice and Public Safety
California University of Penn	MS in Homeland Security
	MS in Cybersecurity
Eastern Kentucky University	MS in Safety, Security, and Emergency Management
Georgetown University	MA in Security Studies
	MA/Ph.D. in Security Studies/Government
George Washington University	MS in Security and Safety Leadership
John Jay College	MS in Protection Management
	MS in Security Management
	MPA-MS in Public Policy and Protection Management
John Madison University	MS in Information Security
Long Island University at Riverhead, Homeland Security Management Institute	MS in Homeland Security Management
Missouri State University	MS in Defense and Strategic Studies; MS in Cybersecurity; MPS in Homeland Security; MS in National Security
National Defense University, The College of International Security Affairs	MA in Strategic Security Studies
New Jersey City University, College of Professional Studies	MS in Professional Security Studies
Southwestern College	MS in Security Management
University College	MAS in Security Management
	MAS in Organizational Security
University of Denver	MA in Homeland Security
	MA in Security Management
	MAS in Security Management, Information Security
University of Detroit Mercy	MS in Security Administration
University of Houston Downtown	MA of Security Management for Executives
University of Maryland	MS in Counter Terrorism and Security
	MS in Cybersecurity
University of Nevada, Las Vegas	MS in Business Continuity, Security, and Risk Management
Virginia Commonwealth University	MA in Homeland security and Emergency Preparedness
Webster University	MA in Business and Organizational Security Management

knowledge and skills from different areas (e.g., Government/Public Management and Security). One way graduate programs do this is by adding a leadership and business continuity component, enforcing public and private sector comparisons and contrasts. These comparisons and contrasts within the curriculum often culminate to an understanding of how an organization permits and sustains growth. Students may learn that without the business side of security, a firm that supplies these services may not be able to benefit and reap rewards.

Another way to improve their expertise in this field is incorporating a major research component into a graduate program for students to delve into a particular phenomenon or problem. Most of these perceived problems pertain to the current state of security in today's society or at least one major area of it. The end result and objective, by in large, will be to create the skill set to defend a thesis or dissertation relevant to their research. Research is data-driven, and security is one major industry which has adopted many data-oriented deliverables within an organization.

Training programs have a different focus than do academia. Agencies and organizations conduct evaluations and assessments on risk, and an abundance of this risk exists in the area of human error. Unbeknownst to many people who work outside the field of security or those who are removed from any scenario in which security is a necessity, programs exist which mission is to spread the message that they are here to educate and train within all levels of the industry, for instance, the National Association of Security.

Companies (NASCO) work closely with state associations, business groups, contractor organizations, and security organizations on mutual issues of concern. NASCO, in particular, articulated that "their biggest highlight" was the completion of a joint project between John Jay College of Criminal Justice and themselves to create an electronic database of state security licensing laws, regulations, codes, and policies governing the licensure of armed and unarmed security officers.

The database will be continually monitored and updated by John Jay with input from NASCO members (Amitay 2013). As the national leader and voice of the contract security industry, NASCO constantly interacts with Congress, federal agencies, state legislators, regulators, the courts, and the media on a variety of industry-related issues. NASCO continued to work with Senator Pat Toomey of Pennsylvania on a bill that will provide security officer employers with *on-demand* nonstate-based access to FBI checks on officers and applicants (Amitay 2013). This working relationship has stayed consistent on the federal level.

At the state level, there continues to be numerous legislative and regulatory issues and challenges for contract security companies in which NASCO was involved, working directly with legislators, regulators, lobbyists, and state associations. In Maryland, a NASCO supported bill to synch up renewals of firearm permits with armed guard licenses was enacted into law. In Connecticut, NASCO, with the assistance of local legislative counsel, worked to find a legislative or policy solution to the current massive delays in officer licensing related to the FBI check process for security officers. In Minnesota, NASCO worked with the state regulatory agency officials, local NASCO company personnel, and the Minnesota state association to stop at the last minute a bill that would have mandated a single uniform and vehicle color for private security. In the state of Washington, NASCO established a working relationship between NASCO members in Washington and the State regulatory agency to address delays in armed officer licensing (Amitay 2013).

Founded in 1955, ASIS International has promoted itself as a global community of security practitioners, each of whom has a role in the protection of assets – people, property, and/or information [see ASIS in this encyclopedia]. ASIS states "No other organization possesses the vast array of knowledge, expertise, and experience" (p. 1). Furthermore, ASIS "offers a range of education programs, publications, and events to help you thrive professionally, whether you're a young professional or an industry veteran" (ASIS 2018, p. 1). The evolution of ASIS on guard training is very evident from an organizational standpoint. Within their educational programming, ASIS provides course curriculum for security practitioners. Training is delivered through multiple means, including online, face-to-face classes, and live webinars. ASIS courses include "Strategy & Tactics in Crisis Management: From Prevention to Recovery" providing a hands-on workshop to teach security personnel how to "analyze methods to manage and control communication, examine components of a comprehensive workplace violence program, strengthen strategies for protecting brand and reputation, examine crisis recovery and consequence management, and discuss how cybersecurity issues affect crisis management" (ASIS 2018, p. 2).

Conclusion

Expectations for training are often correlated with mandates. In the state of New York, security guard

training requirements, Section 89-G of Article 7A of the general business law, requires all persons engaged in security guard activities to be registered with the New York Department of State (DOS) and to complete all trainings (unless exempt) at schools approved by the Division of Criminal Justice Services (NYS Department of Licensing 2018).

In the very place where the most prolific attack on American soil occurred, in New York, the following training courses are required for security personnel, where security guard (unarmed) initial training requirements are an 8-hour pre--assignment training – a general introductory course – and a 16-hour on-the-job training (OJT), a course relevant to the duties of guards, requirements of the work site, and the needs of the employer. This training must be completed within 90 days of employment as a security guard (NYS Department of Licensing 2018). Annually, training requirements are an 8-h annual in-service training, completed each year. In New York registration is issued for 2 years; therefore, security personnel must complete two 8-h annual in-service training courses within their registration effective and expiration dates to be eligible for renewal (NYS Department of Licensing 2018). One may wonder if this is enough. Regardless, despite one's level of education, based on the ample opportunity in our nation to advance, time will tell if these requirements fit the bill within the training and development genre necessary to uphold industry standards and protect life and property.

Cross-References

- American Society for Industrial Security (ASIS)
- Critical Infrastructure: Government Facilities Sector (GFS)
- Personnel Security: Hiring
- Personnel Security: Recruitment
- Personnel Security: Selection
- Security: Concepts and Definitions
- Security: Contract

References

Alexander, K. L. (2018). Former hospital guard charged in patient's death: 'I don't think I did anything wrong. Retrieved from https://www.washingtonpost.com/local/public-safety/former-hospital-guard-charged-in-patients-death-i-dont-think-i-did-anything-wrong/2018/01/25/e4a96aa4-ff7e-11e7-bb03-722769454f82_story.html?noredirect=on&utm_term=.66f2ad0734b7

Amitay, Esq., S. (2013). The Navy Yard Tragedy: Examining Physical Security for Federal Facilities. National Association of Security Companies (NASCO). Senate Homeland Security and Government Affairs Committee Hearing.

ASIS Online. (2018). Retrieved from https://www.asisonline.org/footer-pages/about-asis

Duncan, J. (2013). GAO: FEDERAL PROTECTIVE SERVICE: Challenges with Oversight of Contract Guard Program Still Exist, and Additional Management Controls Are Needed GAO-13-694. Retrieved from http://www.gao.gov/assets/660/657920.pdf

Gstalter, M. (2018, May 3). Security guard charged with assaulting teenager accused of shoplifting. The Hill. Retrieved from http://thehill.com/blogs/blog-briefing-room/news/387513-video-shows-security-guard-choking-black-teen-accused-of

MBASkool. (2018). Human resources. Retrieved from https://www.mbaskool.com/business-concepts/human-resources-hr-terms/8685-training-and-development.html

New York State Department of Licensing. (2018). Retrieved from https://www.dos.ny.gov/licensing/securityguard/sguard.html

Parfomak, P. W., & Library of Congress. (2004). *Guarding America: Security guards and U.S. critical infrastructure protection*. Washington, DC: Congressional Research Service.

Perry, R. H. (2016). *White paper on the U.S. contract security industry*. Accessed at: https://www.robertheperry.com/uploads/2016WhitePaper.pdf. (5.1.19).

Smith, G. B. (2018, May 29). Private security firms as homeless shelters facing 21 lawsuits over alleged violence. New York Daily News. Retrieved from http://www.nydailynews.com/new-york/private-security-shelters-facing-21-lawsuits-violence-article-1.4014201#

Statista. (2018). Security services industry in the U.S. – statistics & Facts. Retrieved from https://www.statista.com/topics/2188/security-services-industry-in-the-us/

Further Reading

Schuilenburg, M. (2015). *The securitization of society, crime, risk, and social order*. New York: New York University Press.

Wood, J., & Shearing, C. (2007). *Imagining security*. Devon: Willan Publishing.

Security Guards: Authority and Power

Christopher A. D. Charles
Department of Government, University of the West Indies, Mona, Jamaica

Keywords
Security guards · Roles · Function · Regulations · Authority · Power

Definition

A security guard is a private citizen employed by individuals and organizations to protect the life of these persons: their staff, their clients, and their property.

Introduction

Although there is a general decline in crime in developed countries in Europe and North America, there has been an increase in the number of private security providers because of the reassurance paradox. This paradox reveals that there has been an increase in perceived victimization as the general risks of crime has declined. The anxiety and fear emanating from this paradox suggests that the rise in private security may have to do more with generalized feelings of societal insecurity rather than the crime rate. The opposite is the case in Latin America and the Caribbean where the discourse of insecurity is more reality than perception because the region has the highest rates of homicides and other violent crimes in the world. Security in developed and developing countries has been dubbed a societal priority hence the need for greater private security (van Steden and de Waard 2013).

The number of security guards tends to be three times the number of law enforcement officers and they provide a critical and crucial security support to law enforcement agencies especially since the 9/11 terrorists attack against the United States. This is evident in the United Kingdom where the police have co-opted private security and have held joint drills with them, among other security and emergency institutions, to better respond to terrorists attacks, and other national emergencies. Both the police and private security believe that such partnerships are beneficial but each group believe that the other could do more to enhance the partnership. This public-private security partnership, which experiences tension sometimes over working relationship and accountability, has nevertheless expanded the society's security architecture. The partnership has also reshaped the structure and function of modern policing. Private security companies have also penetrated new markets overseas and are now part of a global security industry with multinational companies (Cohen 2004; Nalla and Critchlow 2017; Lopes 2018; Shearing and Stenning 1983; van Steden and de Waard 2013).

The jobs held by security guards are generally considered low paying and hence low status jobs. The status of these jobs depending on the country is further exacerbated by societal cleavages based on race, ethnicity, skin color, gender, level of education, and social class. Despite these pejorative contexts, security guards derive their power and authority from several sources. Authority as used here denotes the right to give instructions and exercise control, and power means the influence or capacity to enforce compliance. Employers invest power and authority in the security guards that they employ to secure their property and government regulation of the security industry all of which enhances the legitimacy of security guards. Their authority and power also comes to a lesser extent from the important roles and functions in which they perform comparable tasks to the police services, the security partnerships built with law enforcement agencies, and the perceived positive impact of their work on crime reduction and enhanced societal security (Nalla and Critchlow 2017; Schnabolk 1982; Shearing and Stenning 1983).

Types of Security Guards, Their Roles, and Functions

There are several types of private security personnel. Some of these are residential guards, private guards, patrol guards, business guards, stationary guards, plainclothes guard, uniformed guards, contract guards hired through a private company, proprietary guards that are hired directly, unarmed guards, and armed guards. These guards work in a range of domains such as federal government ministries, agencies and departments, schools, universities, public housing projects, private homes including gated communities, non-gated communities, and state and city agencies, private corporations including financial institutions, malls, and not-for-profit organizations. They also work in religious institutions, entertainment, recreational and sporting events, nuclear facilities, disaster zones, airports, seaports, and on public transportation, airplanes, and commercial ships to prevent piracy on the high seas (Nalla and Critchlow 2017; Petrig 2013; Shearing and Stenning 1983).

Security guards' duties are wide ranging and they have the authority and power (similar to that held by private citizens) to respond to illegal activities at the workplace. The major duties depending on the type of organization are providing information to clients about procedures, and the services and products offered; controlling traffic flow in the workplace by directing motorists; sounding the alarms when necessary to get help; effective use and monitoring of surveillance technology and equipment; periodically inspecting equipment, points of access, buildings, and allowing entry to clients; searching departing clients and staff; patrolling the facility thereby securing staff, clients, and the property; stopping trespassers; and informing those who break the rules of organizational policies and procedures (Lopes 2018; Schnabolk 1982; Shearing and Stenning 1983).

Other duties include documenting and reporting irregularities discovered; providing forensic services; preventing loss and damage to facility; environmental maintenance through the setting and controlling of equipment and buildings including preventative maintenance; assessing new equipment and contacting repair services; following the requirements of the law in support of the reputation and stability of the organization; participating as a cohesive team member to produce outputs; investigations; writing reports of observations, evaluations, and breaches including the recording of witness statements (van Steden and de Waard 2013; Lopes 2018; Schnabolk 1982; Shearing and Stenning 1983).

Public and private organizations invest their security guards with the authority and power to carry out the foregoing roles and functions on their private property within the rule of law (Petrig 2013; Schnabolk 1982). For example, increasing theft in the workplace has influenced some corporations to ask security guards to search customers and staff leaving the premises. This request which is within the rights corporations have to protect their property have to be balanced against the rights of individuals to privacy. Some countries, e.g., Brazil legislate and regulate the powers of search that security guards have at the workplace (Lopes 2018). There are several advantages and disadvantages that have developed as security guards leverage their authority and power in the workplace on behalf of their employers in the service of profits (Schnabolk 1982; Shearing and Stenning 1983; van Steden and de Waard 2013).

Advantages and Disadvantages of Security Guard Work

There are several advantages. The presence of private security in partnership with the police increases societal capacity to control insecurity particularly crimes, terrorism, and other security risks. The pluralization of policing facilitates coordinated synergy between the police and security guards that enhances the security network infrastructure, as well as improved information gathering and sharing. There is also the civiliani-

zation of policing with security guards taking over soft policing roles such as directing traffic, taking emergency calls, serving warrants, and escorting prisoners thereby freeing the police to engage in hard policing and traditional forms of policing. The private security presence also provides competition to the police services that tend to increase performance evident in reduced response time to calls from citizens and increases in the quality of service to the public. Private security services thrive in the market that has limited governments and as such are more adaptive to the changing crime ecology, the new types of crime, and the use of new technology compared to the police. Moreover, private security vendors offer client-oriented services compared to the police where security guards are expected to produce surplus value (Cohen 2004; van Steden and de Waard 2013; Lopes 2018; Nalla and Critchlow 2017; Shearing and Stenning 1983).

Other advantages are that security guards are seen as major contributors to the crime decline. These guards are considered the first line of defense. Therefore, these private security personnel as such are viewed as guardians in the community that produces safety with very little civil liberty problems. Moreover, they have turned gated communities into zones of risk suppression. Security guards' uniformed presence also increases people's feelings of safety especially in unsafe contexts. It is also important to note that private security service users tend to rate the interpersonal competencies of the guards highly compared to the guards' rating of themselves. Security guards have also been hailed as heroes for their help in emergencies like floods and fires and so on. These advantages influence many members of the public to view security guards positively with increased confidence based on increased trust and satisfaction with them. However, Whites held more negative views about security guards than Blacks. Also, lower income individuals compared to middle class persons prefer security guards compared to the police (Nalla and Critchlow 2017; Schnabolk 1982).

The disadvantages associated with the work of security guards undermine their authority and power. Competition in crime and security can undermine the public-private security partnership reducing the effectiveness of the overarching security network. Blurred operational lines between private and public security sometimes occur leading to public governance through private security. This occurrence is a threat to democracy. Moreover, some private security personnel are associated with paramilitary violence and the accountability system for the private security industry is inadequate (van Steden and de Waard 2013).

Countries are moving towards the creation of a greater disciplinary society with greater private security to protect property rights that have led to threats to individual liberties. The police, for example, have arrested and charged some security guards for rape, assaulting customers, or the use of excessive force, theft, drug use, facilitating drug transactions, false imprisonment, and shooting people in the back. Other security guards have been accused of attacking psychiatric patients, discriminating against minorities leading to lawsuits, and failing to respond to reported crimes and so on. As such, some people hold negative views of security guards because some have not been compliant with the stated demands of private security vendors (van Steden and de Waard 2013).

Some of the disadvantages of private security that have been identified above may be addressed in several ways. These are that security guards should receive better education and training, they should have better amenities at work, also better work schedules, receive livable wages, health insurance and pension, and be provided with ongoing corrective feedback about their performance (Cohen 2004; Hemmens and Klein 2018). Dealing with the foregoing should increase the security guards' job satisfaction and reduce the high rate of job turnover. Governments tend to respond to these problems, the crime concern and the respect for civil liberties by regulating the private security industry (Lopes 2018).

Regulating Security Guards

There are generally regulations governing security guards that vary based on country with developed countries having more regulations than developing

countries. These regulations are of critical importance because private security firms perform comparable functions to the police. In the case of the United States, approximately 90% of the states have some regulations governing private security in the absence of federal guidelines. These requirements for hiring security guards are designed to protect the public. The push to professionalize the private security industry and make it adaptable to challenges has been unremarkable in some countries. However, the overall push has made the industry more accountable which has given it more legitimacy with citizens (Hemmens and Klein 2018; Lopes 2018; Nalla and Critchlow 2017).

Most states in the United States have licensing requirements for security guards but there are none in Missouri, Mississippi, South Dakota, Colorado, and Idaho. Some 84% of the states require a criminal record check for security guard applicants with 64% of the states requiring proof of citizenship or permanent residency status, 45% requiring training for unarmed guards, and 12% requiring training for armed guards. For the latter category of guards, 84% of the states have a minimum age requirement. The states that did not have specific armed training requirements for security guards relied on the firearm licensing laws of the state. Although training of security guards is largely neglected in the country, the states of California and New York have made training and oversight mandatory. Only 29% of states have a minimum education requirement for guards with only 10% requiring applicants to sit a written examination (Hemmens and Klein 2018; Nalla and Critchlow 2017).

Private Maritime Security: Security guards working on board ships for private maritime security companies to counter piracy on the high seas are a challenge to the notion of the navy and the coastguard having responsibility for maritime security. Naval presence is important but it is not necessarily a deterrent to piracy. Shipping companies have two choices. The first is the use of private maritime security companies and the second is the use of vessel protection detachments that are small teams of security personnel on board the ship acting in their capacity as state officials serving as police or military personnel. The latter have the right to use force as agents of the state. Although companies have a preference for state officials, there is limited resources so some civilian companies use private security guards. Therefore, some countries have started to review their legislations to allow the use of private security guards on commercial ships (Hemmens and Klein 2018; Petrig 2013; Schnabolk 1982).

Some of the rules governing private maritime security states that these guards should always have access to maritime legal advice because the position of the armed guards are not precise under international law and the domestic laws of countries. The laws dealing with carrying and using guns on board ships along with other security equipment are sophisticated. The laws of the flag State govern guns and armed guards on ships traversing the high seas. The country to which the ship is registered is the obligated state under international law to prescribe and enforce rules. Maritime security guards may also be obliged to follow the laws of the country in which the company is incorporated. Therefore, a commercial ship using armed private security personnel and going through a third state's territorial waters, or using a foreign state as a port of call, is expected to comply with the laws on the use of firearms in the coastal and port states that may differ from the gun laws of the flag State. The maritime security guards derived their authority and power at sea from their employers and applicable laws similar to their counterparts working on land (Hemmens and Klein 2018; Petrig 2013; Schnabolk 1982).

Conclusion

There has been the globalization of private security companies employed in organizations ranging from schools to public transport and companies whose ships traverse the high seas and companies in response to the perceived rise in crime, terrorism, and other security risks. Security guards and the new technology they bring in client-oriented services in the market have led to fruitful partnerships with law enforcement agencies despite the occasional competition and tensions. Private security companies are now an important part of the security structure in the modern world. Their

authority and power are largely derived from their contracts to protect people and their private properties and the state regulations governing private security companies that enhances and legitimizes them. They also emanate from the important security roles and functions they perform in society, their security partnerships with the police, their perceived role in the crime decline, and enhanced security. Therefore, the post 9/11world now has plural policing comprising strategic public-private security partnerships buttressed by the support of citizens that have changed the nature of security in the modern state system.

Cross-References

- ▶ Arrest
- ▶ EU Private Security Regulation
- ▶ Event Security
- ▶ Investigations: Employee Theft of Employer Property
- ▶ Maritime Security: Armed Guards on Board
- ▶ Police: Public Versus Private Policing
- ▶ Retail Security: Use of Security Guards
- ▶ Security Guards: Authority and Power

References

Cohen, L. M. (2004). Keeping chaos under control. *Security Management, 48*, 80–88.

Hemmens, C., & Klein, M. S. (2018). Public regulation of private security: A statutory analysis of state regulation of security guards. *Criminal Justice Policy Review, 29*, 891–908. https://doi.org/10.1177/0887403416649999.

Lopes, C. D. S. (2018). Policing labor: The power of private security guards to search workers in Brazil. *Crime, Law and Social Change, 70*, 583–602. https://doi.org/10.1007/s10611-018-9783-x.

Nalla, M. K., & Critchlow, V. J. (2017). Have the standards for private security guards become more stringent in the post 9/11 era? An assessment of security guard regulations in the US from 1982 to 2010. *Security Journal, 30*, 523–537. https://doi.org/10.1057/sj.2014.21.

Petrig, A. (2013). The use of force and firearms by private maritime security companies against suspected pirates. *International and Comparative Law Quarterly, 62*, 667–701. https://doi.org/10.1017/S002058931300016X.

Schnabolk, C. (1982). The legal basis of authority. *Security Management, 36*, 50.

Shearing, C. D., & Stenning, P. C. (1983). Private security: Implications for social control. *Social Problems, 30*, 493–506.

Van Steden, R., & de Waard, J. (2013). 'Acting like chameleons': On the McDonaldization of private security. *Security Journal, 26*, 294–309. https://doi.org/10.1057/sj.2013.18.

Further Reading

de Waard, J. (1999). The private security industry in international perspective. *European Journal on Criminal Policy and Research, 7*, 143–174. https://doi.org/10.1023/A:1008701310152.

Parfomak, P. W. (2004). *Guarding America: Security guards and U.S. critical infrastructure protection*. CRS report for Congress. https://apps.dtic.mil/dtic/tr/fulltext/u2/a454027.pdf

Sarre, R., & Steden, R. V. (2007). The growth of private security: Trends in the European Union. *Security Journal, 20*, 222–235. https://doi.org/10.1057/palgrave.sj.8350052.

Security Management

Robert McCrie
Deptartment of Security, Fire and Emergency Management, John Jay College of Criminal Justice, New York, NY, USA

Keywords
Security · Protection · Management · Risk mitigation

Definition

Security management is the administration of a program that protects or reduces assets from loss.

Introduction

Security management is the administration of a program that protects or reduces assets from loss. In an earlier era, the definition of security frequently used was "private people protecting

private property." That early characterization was in decline by the turn of the twenty-first century and became obsolete following the terrorist attacks of 9/11. Those attacks affirmed the role of security as a private resource but one that also suggested a duty to reasonably aid the public within its limited sphere of influence (IACP and COPS 2004; McCrie 2016).

A Discipline in Development

Security in the context of this discussion means secure, safe, and free from care. It embodies the concept of safety and freedom from worry and danger. The word *management* comes from Middle Age derivatives of the French *ménagerie* (housekeeping, including animal care, especially horses) and the Italian *maneggiare* (to handle, especially tools or a horse). This artisanal and barnyard word origin belies a serious responsibility not so discernible in contemporary use: administering property and taking care of horses – the most valuable and useful domestic animal in earlier centuries – required knowledge, commitment, and reliability.

Without management, progress would be stuck; the fruits of civilization would be blocked from flourishing. Humankind has achieved grand objectives first by planning and then managing the plan to reach the goals that were decided upon. Through management, past civilizations created the precisely engineered pyramids, the Great Wall of China as well as city walls throughout the developed world, vital aqueducts and road systems, military fortifications and structures, and inventions that could make products in quantity and for less cost than low-production handcrafted methods of the past. Management's objectives do not relate exclusively to the concerns of structures or manufactured goods. Effective management also encompasses functional strategies for achieving countless other physical and operational achievements that embody the human spirit in striving for a safer, richer, better life. None of these achievements could have occurred spontaneously out of chaos and disorganization. People alone turned dreams into systematic concepts and then organized the resources to achieve their ultimate objectives.

Yet general management, as an academic discipline and subject of critical analysis, is just about a century old. The Wharton School began in 1881 with an undergraduate focus. The emergence of graduate schools of business administration created a further emphasis on identifying what makes organizations succeed or fail (Cruikshank 1987). The contributions of classical management provided a framework for thinking about management with the writings of Henri Fayol. Classical management exponents concentrated on production and predictability: Frederick Winslow Taylor, Frank and Lilian Gilbreth, and Henry L. Gantt. Early on, the case history method became a core strategy of examining strengths and weaknesses of actual organizations, probing their strengths and weaknesses, and challenging student analysts to find a productive way ahead (Heath 1998; Cummings 2017). Future executives and senior managers learned to set the strategy and amass the resources to meet the expectations of capital providers, institutional visionaries, and government functionaries. But what about security management?

We argue that security is the first necessity of any organization (McCrie 2006). Without protection of assets, work cannot be accomplished with certainty, plans cannot be assured, and creativity may be squandered. Not every workplace requires a security manager or an articulated program. A great many workplaces have common sense protective measures as part of their organizational DNA, and conventional security responsibilities are dispersed within them widely. Similar to early management practitioners, contemporary security managers concentrate on collecting and assessing activities related to their responsibilities to improve plans and programs. All organization have the challenge and duty to protect assets from loss, and as organizations expand in size and complexity, the utility of having timely practices and knowledgeable managers to mitigate losses increases, especially for cybersecurity, protection of intellectual property, and executive protection.

Security management became recognized as a distinctive discipline, gradually emerging as a topic for research and teaching during the Cold War era

and drawing from teaching and research in graduate management education. A starting point was the organization in 1955 of the American Society for Industrial Security, now ASIS International (McCrie 2005). A handful of security directors, most with government-issued security clearances, first met in Los Angeles, to discuss challenges in protecting the critical national activities they performed for the federal government. Quickly, security directors in other industrial and commercial sectors, and those with related responsibilities, sought this forum to associate with practitioners to share views and obtain information vital to the conductance of their individual activities. They wanted in. The new organization began to grow. Currently, ASIS International claims 35,000 members in over 240 chapters around the world. However, as managerial interests expanded and became more specialized, literally scores of trade and professional organizations could be identified that serve various loss mitigation and recovery activities (Security Letter 2017).

The process of security management continues to evolve, but two fundamentally different tasks are apparent. Management skills are needed to administer ongoing programs or endeavors. That is, the manager continues to direct with appropriate change what has already been ongoing. But a distinctive set of management skills is required to launch new projects or programs. The sequence of this planning process involves sequential and interlocking progression that is applicable to security planning as well as general management endeavors:

Setting the Goal

Leaders decide what existing program needs to be administered or what new initiative must be set for the organization to move forward. Someone is appointed to be in charge.

Gathering the Information and Analyzing it

The new venture to be managed well needs to be planned using all relevant data sets and experiences. In a security program, such information must be considered like crime trends, available police and emergency resources, past relevant incidents, physical location of the entity for which the plan is being created, personnel required, technical skills needed, and numerous other factors. The security planner or planning team then meticulously envisions the end result and identifies the resources needed and timeline requisite for achieving the goal. This flows into the next step.

Organizing the Plan

The manager looks toward the ultimate goal and allocates funds and human resources toward fulfilling the plan. Depending on the complexity of the objective, the time required can be as little as a few hours to many months of concerted activity by a team. The process of planning brings together the totality of the organization's resources, including personnel skills, technology, industry trends, laws and regulations, and available financing to make the plan achieve its objectives. The plan becomes ready to launch, though remains flexible to changing circumstances.

Deputizing Someone to Manage the Plan Once the Plan Is at an Advanced State

The initial planner might be responsible for managing the resultant new plan that is in place. But in many cases, particularly in complex organizations, a member of the planning team is selected to take personal responsibility for managing what has been created. The plan has moved from the realization of a need to the formation of a strategy to operate and manage what has become the organized, financed, staffed, and supported operation that will continue and hopefully bring desired results. This phase being completed, the senior manager normally allows the subordinate to assume the authority linked to responsibility for working toward achieving the agreed-to programmed objectives.

Supervising the New Manager

In this scenario the initial head of planning supports the subordinate in achieving the established goals of the process.

Constant Program Revision and Enhancements

A program once created is likely to undergo nuanced changes with experience of the ongoing plan. This is a normal expectation in security management due to incessant change of circumstances.

This process with analyze-organize-deputize-supervise at its core is the mantra for high-performing security managers as well as managers with different organizational responsibilities.

Through this process, security management seeks to provide relevance to organizations by reducing constantly evolving risks, responding to emergencies and disasters, meeting legal requirements, working with other managerial entities, and protecting organizational capital, resources, and reputation.

Conclusion

Risk occurs in all organizations and constantly evolves. Its reduction is a function of management that links controls to the identified risk. Security management can be practiced in small organizations by a single individual working on an ad hoc basis to a complex program employing thousands and with a budget in the nine digits. The manager in charge begins with collecting relevant information to create the operational plan. Then, the steps needed are organized for action. Someone is placed in charge to manage the new plan, and the senior manager supervises the ongoing fulfillment. Yet, security management is a dynamic activity, and new issues arise regularly, requiring the management protocols to be adjusted.

Cross-References

- ▶ Corporate Security
- ▶ Critical Infrastructure Protection
- ▶ Data Protection
- ▶ Emergency Management: Preparedness and Planning
- ▶ Internet of Things
- ▶ Security: Concepts and Definitions

References

Cruikshank, J. L. (1987). *A delicate experiment: The Harvard Business School, 1908-1945*. Boston: Harvard Business School.

Cummings, S. (2017). *A new history of management*. Cambridge, UK: Cambridge University Press.

Heath, J. (1998). *Teaching and writing case studies: A practical guide*. Bedford: European Case Clearing House.

IACP and COPS. (2004). *National policy summit: Building private security/public policing partnerships to prevent and respond to public disorder*. Alexandria: International Association of Chiefs of Police.

McCrie, R. (2005). ASIS international. In L. E. Sullivan (Ed.), *Encyclopedia of law enforcement* (Vol. 2, pp. 547–549). Thousand Oaks: Sage Publications.

McCrie, R. (2006). A history of security. In M. Gill (Ed.), *Handbook of security*. London: Palgrave Macmillan.

McCrie, R. (2016). *Security operations management* (3rd ed.). Waltham: Butterworth Heinemann.

Security Letter. (2017, May–June). Directory of leading security organizations, Part II.

Further Reading

Martin, G. (Ed.). (2014). *Handbook of security* (2nd ed.). London: Palgrave Macmillan.

Sullivant, J. (2016). *Building a corporate culture of security*. Waltham: Butterworth-Heinemann.

T

Terrorism: Domestic

Arie Perliger[1] and Matthew M. Sweeney[2]
[1]School of Criminology and Justice Studies, Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA
[2]School of Criminology and Justice Studies, University of Massachusetts Lowell, Lowell, MA, USA

Keywords
American Far Right · American Far Left · US terrorism · Anarchism · Environmentalism · Jihadism in America

Definition

Academics and policymakers designate politically violent attacks perpetrated within the US territory, by groups, which are mostly based in the United States as (American) domestic errorism. The American Federal Bureau of Investigation (n.d.) defines domestic terrorism as acts "perpetrated by individuals and/or groups inspired by or associated with primarily U.S.-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature."

Introduction

However, such a definition can also lead to the inclusion of groups which while are based in the United States operate in a context of a foreign conflict. For example, when presumably Palestinian militants assassinated Yosef Alon, the military attaché to the Israel Embassy in DC in 1973, it was clear to the FBI that the assassination was in the context of the Israeli Palestinian conflict (TOI Staff 2017). Hence, it is conceptually useful to add that local groups in US territory do not just perpetrate domestic terrorism, but these groups may also perpetrate attacks in the context of local political or social conflicts.

Probably the first American group which engaged in a continuous campaign of what can be defined as domestic terrorism emerged in 1865 when former officers in the Confederate Army formed the Ku Klux Klan in Pulaski, Tennessee (McVeigh 2009; McVeigh et al. 2004). While the first Klan lasted for only a brief period, American political, religious, and Nationalist groups continue to engage in campaigns of terrorism to promote their ideological objectives. The main reasons for the emergence of these groups, their ideological foundations, and their operational characteristics will be the main focus of the discussion in the following sections. After discussing violent manifestations from the American Far Right, including racialist, anti-federalist, and fundamentalist groups, we will

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

address the violentgroups which originated from the American Far Left, to include also anarchists and environmentalist extremists. Subsequently, we will examine the jihadist movement in the United States, as well as analyze domestic ethnic and ethnonationality violent movements. We will conclude with a comparative overview of the main features of domestic terrorism in the United States.

American Far Right

The American Far Right is highly diverse and fragmented. It is characterized by significant ideological diversity (as different groups emerged from distinct cultural traditions), organizational instability (frequent merges and splits), as well as various operational methods, as different groups prefer to use different tactics against different types of targets. Nonetheless, two dominant ideological tendencies seem to be shared by most American Far Right groups. The first is the aspiration that all residents or citizens of the polity/community will share the same ethnic, religious, and national characteristics. This desire for internal homogenization led many American Far Right groups to emphasize that contemporary social, economic, and political crises are resulting from the inability of modern societies to implement this principle. For example, in 2016, the Californian "Loyal White Knights" was involved in a series of violent protests which linked immigration, terrorism, and street crime (Queally 2016). The second ideological element which is shared by most far-right groups in the United States is opposition to foreign influence and the rejection of non-native cultural, religious, and normative practices. Thus, they oppose the assimilation of non-American holidays/costumes, social behaviors, art, linguistic phrases, musical themes, etc. They consider foreign influence as a threat to the ability to maintain what they consider American heritage, a way of life, and exceptionalism (Rice 1972). In this context, many of them also exhibit practices of xenophobia and racism and promote various *exclusionary* policies.

Despite the complex nature of the American Far Right, scholars have divided it into three major streams, which have unique ideological origins and specific operational and organizational characteristics (Durham 2000, 2003; Perliger 2012). The first is the racialist stream, which asserts that Americans of European ancestry, particularly those from Northern Europe, are superior to people from other parts of the world. Adherents believe that "white" people should maintain control over social, economic, and political domains in the United States, and people from other ethnicities and racial groups should not integrate with white people (Barkun 1997; Perliger 2012). This desire results in ideological beliefs which correspond to nativism, racism, and xenophobia.

Three types of movements dominate the racialist stream: the Ku Klux Klan, Nationalist Socialist Movements, and the American Skinheads (Perliger 2012). The Ku Klux Klan has a long history, disbanding and rebranding itself numerous times throughout the twentieth century (McVeigh 2009; Perliger 2012). Although each emergence of the Klan was characterized by a new set of tactics, membership criteria, and organizational structure (McVeigh 2009), its ideology maintained its focus on preserving racial segregation and opposition to legislation and policies which aimed to ensure racial equality in various spheres of society. Local Klan chapters mainly emerged in locations where white protestants were the overwhelming majority and maintained some level of independence (McVeigh 2009; McVeigh et al. 2004), even though the movement was governed until the late 1940s by a national hierarchal structure led by the Grand Wizard. The Ku Klux Klan saw its height in the early twentieth century. However, after significant attention from law enforcement and legislation, Klan organizations rapidly declined in the late 1960s and early 1970s century. This crisis opened the door for the rise of new and young leadership, which in the 1970s and 1980s, adopted the white supremacy rhetoric. David Duke, at that time one of the emerging leaders of the KKK, described this transition as a move from the "cow pastures" to the "hotel meeting rooms" (Wade 1987, p. 368).

This phrase reflected the transition from a language focusing on degrading other ethnic or religious groups to a protectionist language focusing on the need to protect the civil rights and heritage of the white people while also asserting that segregation and exclusionist policies will also benefit non-white groups. The group's reforms did lead to some rise in the Klan's membership, the resurgence was minimal, and today most KKK chapters throughout the United States are small and inconsequential, commonly appearing in news media for their attempts to recruit new members (for example, Craig 2018; Hafner 2018; Nero 2018).

The Nationalist Socialist Movement first emerged in the 1930s and 1940s in response to the rise of Nazism in Germany. However, the movement remained small and failed to gain traction despite the charismatic leadership of George Rockwell, the formal leader of the American Nazi Party in the 1950s and 1960s. However, in the second half of the 1970s, the National Socialist Movement finally gained significant ground, via the National Alliance, the most violent and well-organized neo-Nazi organization in the United States (Southern Poverty Law Center n.d.). The National Alliance was responsible for the expansion of Resistance Records, a Neo-Nazi music company which, at its height, had an annual income of over $1,000,000 (Southern Poverty Law Center n.d.), as well as able to mobilize support from various facets of American society effectively. However, National Socialism began to decline in the 1980s due to the aging of its membership and the growing challenge to recruit a new generation of activists. One of the reasons for this challenge was the emergence of a new, youth-centered subculture, which its members where known as Skinheads.

The Skinhead Movement originated in the 1970s in the United Kingdom as a movement which rejected the free-thinking hippie movement, attracting white, working-class youth (Pollard 2016; Southern Poverty Law Center 2012). While racism and neo-Nazi ideology were not always synonymous with Skinheads, racist organizations dominate the American Skinhead subculture which started to proliferate in the early 1980s. American skinheads groups relied on economic and social anxiety to mobilize young, uneducated, white Americans (Perliger 2012) who were attracted to Skinheads propaganda which blamed globalization and increasing immigration for the difficulties of working-class white Americans (Pollard 2016; Southern Poverty Law Center 2012). Initially, the skinhead movement lacked any central coordination, but during the 1990s, most Skinhead organizations eventually became affiliates of the Hammerskin Nation, the largest and most well-organized Skinhead organization in the United States (Anti-Defamation League 2005a, b; Perliger 2012). The organization continued to evolve – developing a national headquarters and international affiliations – until the late 1990s and early 2000s, when it began to fracture, resulting in the creation of independent Outlaw Hammerskins groups (Anti-Defamation League 2005b). Currently, the Hammerskin Nation maintains a popular online community and has international affiliates. Collectively, National Socialist and Skinhead organizations are known as the White Power Movement, along with others in the racialist stream (Blee 2002; Dobratz and Shanks-Meile 1997; Simi and Futrell 2010).

The second stream of the American Far Right is the anti-federalist movement, which is a new phenomenon compared to the long history of racism in the United States. The anti-federalist movement emerged in the 1970s "based on the idea that there is an urgent need to undermine the influence, legitimacy, and practical sovereignty of the federal government and its proxy organizations" (Perliger 2012, p. 28). Anti-federalists embrace three central views. The first is that there is a concerted effort by the US Government to strip Americans of their rights (Belew 2018). The second implicates a larger shadow government poised to overthrow the US Government and institute a "New World Order" under the control of the United Nations (Pitcavage 2001). Lastly, some adherents promote anti-Semitic conspiracies of a Zionist Occupied Government, known as the ZOG, in which a worldwide Jewish conspiracy controls the US Government (Dobratz and Shanks-Meile 1997;

Durham 2003; Simi and Futrell 2010). While these beliefs do not apply to all anti-federalist organizations, all of the organizations promote the idea that the US Government is already corrupt or highly influenced by foreign actors who facilitate its corruptive nature (Perliger 2012).

The anti-federalist stream includes a variety of tax protest, anti-government, and militia groups. Tax protesters have never gained significant attention in the United States, and most shun violent acts against the US Government. One of the few anti-taxation organizations which garnered substantial support was the Posse Comitatus. The Posse Comitatus was active from the early 1970s through the 1980s. It combined anti-tax ideas with mild racialist sentiments and rationalized the illegality of federal taxes by asserting that the only legitimate form of governance in the United States existed at the county level. Additionally, the Posse Comitatus capitalized on the 1980s farm crisis and the insecurities of poor, rural, white Americans who felt a decline in their social status to spread fears of an overreaching government and a collapsing rural economy (Audsley 1985; Levitas 2002). In this context, the Posse Comitatus actively promoted conspiracy theories regarding paper money. They offered fraudulent paper checks to farmers to repay their loans and argued that since the bank paid the farmer with a check, the farmer could repay the bank with any paper check, regardless of its validity. As the Posse Comitatus' financial tactics failed, they resorted to violence to defend family farms and to counter attempts by the IRS to enforce federal tax laws. The most notable violent incidents occurred in 1983 when Gordon Kahl, a member of the Posse Comitatus, killed two federal marshals who attempted to arrest Kahl for tax evasion (Levitas 2002). While the Posse Comitatus dramatically declined in the mid-1980s, the organization laid the groundwork for future tax protest and anti-government organizations, including the Sovereign Citizen Movement.

The Sovereign Citizen Movement, also known as *Freeman on the Land*, and similar terms, expanded rapidly after the housing collapse and the great recession which the United States experienced in 2008. Sovereign citizens are "anti-government extremists who believe that even though they physically reside in [the United States], they are separate or 'sovereign' from the United States." Ideological adherents often refuse to pay taxes and to recognize or cooperate with public officials. Another common tactic is the filing of fraudulent tax returns to recoup the money they believe the US Government is holding under their name (a belief which is an outcome of a standard conspiracy theory among sovereigns, known as redemption theory) (Berger 2016b). Beyond financial-based crimes, sovereigns account for more than 40% of financial crime associated with the American Far Right (Sullivan et al. 2015); some sovereigns also engage in violent practices, mainly against proxies or representatives of the federal government. Between 2000 and 2016, sovereign citizens were responsible for the deaths of 18 law enforcement officers and 9 civilians and for the injury of 17 law enforcement and 9 civilians (MacNab 2017). While sovereigns are currently more popular than other anti-federalist movements, they maintain a much more decentralized structure and seem to be less coordinated, hence mainly operating independently.

In the early 1990s, militia organizations existed in all 50 states. This trend reflected the growing distrust of the United States federal government as a result of declines in family-run farms and declines in industrial jobs for service-based and high-tech oriented jobs (van Dyke and Soule 2002). Most of the militias engaged in military training and produced propaganda material which promoted various NWO narratives. However, some militia members occasionally also plotted violent operations, as a protest against what they perceived as the tendency of the federal government to promote intrusive policies which are contradicting their constitutional rights. The most known such incident was the Oklahoma City Bombing on April 19, 1995, in which the explosion of a Ryder truck bomb outside the Alfred P. Murrah Federal Building in Oklahoma City caused the death of 168 people and the injury of close to 700, and was the second largest terrorist attack in the United States. It was

perpetrated by Timothy McVeigh, who was later linked to a variety of anti-federalist organizations and adopted extreme anti-federal convictions (Belew 2018).

Following the attack in Oklahoma, the federal government and state legislatures acted quickly to limit the organized activities of anti-federalist organizations. While these actions reduced the capabilities of the organizations to conduct training and mobilize support, the legislation did not alleviate the grievances that led to the expansion of the militia movement and other anti-federalist groups (Vertigans 2007). Thus, the militia movement experienced a partial resurgence with the housing collapse and great recession of 2008 and the election of Barrack Obama as the 44th President of the United States. Nonetheless, the movement never regained the same level of popularity it had in the 1990s (Southern Poverty Law Center 2009).

The last stream of the American Far Right includes a variety of religious extremists including Christian Identity adherents and anti-abortion organizations. Christian Identity is a warped subset of Christian theology in which Northern Europeans, not the Israelites, are the chosen people of God (Sharpe 2000). Adherents posit that racial minorities existed before Adam and Eve as soulless mud people, and only Caucasians are in the image of God. Further, they believe that Jews are the spawn of Satan through a relationship between Eve and the serpent in the Garden of Eden (Barkun 1997). While Christian Identity churches and congregations remain small, a variety of organizations have expressed their beliefs and engaged in terrorist attacks throughout the United States. Members of the Covenant, Sword, and Arm of the Lord, a Christian Identity commune, attempted to bomb a natural gas pipeline and had plans to poison a large public water supply in the late 1980s (Noble 2010). Many of these groups believe in a coming racial war, based on the interpretation of *The Turner Diaries*, a racist novel depicting a revolution against a corrupt government controlled by Jews and minorities in the United States (Berger 2016; MacDonald 1978).

The latter part of the Christian fundamentalist stream comprises the extreme portion of a mainstream element of the conservative far-right's agenda against abortion in the United States (Perliger 2012). However, antiabortion groups like the Army of God, a leaderless organization responsible for the deaths of physicians and the bombings of abortion clinics, emphasize the lengths some members are willing to go to stop what they term the "abortion industry" (Munson 2008). Antiabortion activists traditionally present their actions, including violence, as acts which aim to save the unborn children (Winter 2014). The most notable members include Reverend Michael Bray, an outspoken advocate and upporter of violence against abortion clinics and physicians, and Scott Roeder, an activist who shot and killed Dr. George Tiller, a physician known for his willingness to perform late-term abortions, in 2009.

The American Far Right is a significant part of the terrorism landscape in the United States. Perliger (2012) chronicled over 4400 cases of far-right violence and property crime from 1990 to 2012. Further, Sweeney and Perliger (2018) believe that much of the activity occurs spontaneously, without planning or premeditation. Regardless of the perpetrator's planning, the far right has shown considerable prowess in engaging in violence in the United States. Notably, the "alt-right," the newest manifestation of the American Far Right, encourages people to commit acts of violence through online social media platforms (Perliger 2017a, b). Since 2016, the alt-right has staged free speech rallies and pro-President Trump rallies, attracting violent elements of the far right and far left and leading to violent street battles between the alt-right and Antifa, a far-left anti-fascist movement (Swenson 2018).

The American Far Left, Anarchists, and Environmental Groups

The American Far Left includes "groups or individuals that embrace anticapitalist, Communist, or Socialist doctrines and [seek] to bring about change through violent revolution" (Department

of Homeland Security 2009, p. 6). Throughout the twentieth century, the United States experienced multiple waves of far-left terrorism which were promoted mainly by a variety of Marxist and Leninist groups, but occasionally also by anarchists and members of animal and environmental rights groups. While the popularity of these groups fluctuates greatly, far-left terrorism was an acute threat mainly in the 1970s and early 1980s, when it was responsible for three-fourths of all officially designated acts of domestic terrorism (Seger 2001).

Probably the most known American Far-Left group was the Weather Underground, which operated in the early to mid-1970s and was comprised mainly from students from Ivy League universities and engaged in bombing campaigns of FBI offices and other symbols of the federal government (Forest 2012). The organization which was a militant advocate against the Vietnam war and other cold war policies also aimed to increase awareness to American imperialistic, racist policies and the negative impact of consumerism and capitalist doctrine. It eventually faded in 1977 as a result of growing pressure from law enforcement, the end of the Vietnam war, and the decline of the New Left movements all over the globe (Forest 2012).

Anarchism is "a philosophy that advocates for complete liberty, freedom, and equality" without government or the traditional Westphalian concept of statehood (Borum and Tilby 2005, p. 202). In the United States, anarchism has experienced popularity mainly in the early twentieth century, a trend which also was manifested via violent attacks against symbols of the American polity and capitalist system. The assassination of President McKinley in 1904 by an anarchist activist is a case in point, as well as the September 16, 1920 attack in Wall Street, when a cart exploded in front of the J. P. Morgan and Chase Company headquarters in New York City (Federal Bureau of Investigation 2010; Forest 2012). The intended target was J. P. Morgan, whom anarchists viewed as a symbol of capitalism. However, he escaped without harm, which was not the case for the seven fatalities and dozens of injured. The movement's eventual decline later in the mid-1920s was due to a lack of coordinated effort against aggressive government intervention through laws which outlawed anarchist speech (Colson 2014).

Since the mid-1980s, environmentalist and animal rights groups began to increase their activities in the United States. While organizations such as *People for the Ethical Treatment of Animals* and *Greenpeace* primarily operate within the boundaries of the law (Liddick 2014), some other associations preferred to utilize violence and illegal practices. The Earth Liberation Front (ELF) and Animal Liberation Front (ALF) use property damage and acts of harassment and threats against individuals and organizations they believe are abusing animals or destroying the environment to achieve their goals (Liddick 2014). Both the ELF and ALF emerged in the United States in the 1990s and expanded significantly in the 2000s, leading the Congressional Research Service to identify these movements as a leading security threat to the United States (Bjelopera 2013, 2014), especially as they expanded their engagements in acts of arsons, bombings, and property damage (Carson et al. 2012).

Jihadi Terrorism in the United States

Religious terrorists twist the underlying interpretation of religious scripture to justify violence. In the United States, there are many examples of religious terrorism, particularly among the American Far Right, but Islamic Jihadi terrorism has taken the preeminent position in the United States. Islamist extremists use interpretations of Koranic verses to justify their violence as defending Islam, or they interpret the verses as requiring the expansion of Islamic control throughout the world. Traditionally referred to as the global jihadist movement, Islamist extremists have targeted the United States since the 1970s. However, until the 1990s, much of the violence targeted American institutions abroad, and the attacks involved non-US citizens.

In the 1990s, Osama Bin Laden, the former leader of Al-Qaida, issued multiple declarations

of war against the United States for its military presence in Saudi Arabia and the invasion of Iraq during the Gulf War. Following the September 11, 2001 attacks, Al-Qaida and other jihadist organizations have inspired domestic attacks inside the United States. Domestic jihadist attacks involve individuals who did not enter the United States with the purpose of committing an attack, but they became inspired to commit acts of violence for the jihadist cause. In 2009, Major Nidal Hassan, a psychiatrist with the US Army, opened fire on soldiers and civilians at Fort Hood near Killeen, Texas. Hassan killed more than a dozen people before law enforcement wounded Hassan. The resulting investigation revealed Hassan was in contact with Anwar Al-Awlaki, an American citizen and al-Qaida operative in Yemen, who encouraged the attack. The Islamic State has also encouraged attacks in the United States. In 2016, Omar Mateen killed almost 50 people in the Pulse Nightclub in Orlando, Florida. Shortly before beginning his mass shooting, he called law enforcement and pledged his allegiance to the Islamic State. While these are only two incidents, they represent the type of mass casualty attack jihadist ideologies have inspired since September 11, 2001.

Ethnic Terrorism

Ethnic violence in the United States is less common than violence associated with other ideologies. However, two movements have engaged in violence in the United States in the name of an ethnic group or a nationalist goal. The first is Puerto Rican Separatists who seek Puerto Rican independence from the United States, and the establishment of a Marxist or socialist government in Puerto Rico. For example, the Fuerzas Armadas de Liberación Nacional ("Armed Forces of National Liberation"), or the FALN, engaged in multiple bombings, robberies, and weapon violations in the 1980s and is still considered the most prolific terrorist group which ever operated in the United States. In 1980, authorities arrested a dozen FALN members in Illinois on charges of robbery, conspiracy, and weapon violations. The arrests resulted in numerous convictions on a variety of charges, but due to violations of legal practices by the Federal Bureau of Investigations' investigation into the FALN, President Bill Clinton commuted the sentences of 14 FALN members in 1999 (González-Cruz 2008). Today most Puerto Rican Nationalists engage in non-violent activism.

The second movement is the Chicano Separatist Movement, which seeks to claim ndependence for territory known as Aztlán in the Southwestern United States. While the Chicano Separatist Movement has no centralized extremist organizations, single members have engaged in terrorist violence in the United States. For example, in the 1960s, Reies López "El Tigre" Tijerina, leader of the Alianza Federal de las Mercedes ("Federal Alliance of Land Grants"), took two US park service rangers hostage in the Kit Carson National Forest to protest the federal government's transition of lands from the local community into a national forest (Trivett 2014). Tijerina and his followers put the two park rangers on trial for trespassing. Following the trial, federal authorities quickly arrested those involved which led to a downfall in the use of criminal tactics by Tijerina and much of the Chicano Separatist Movement (Trivett 2014). Currently, the movement seeks non-violent and protest activities, focusing on the rights of Latinos in the United States and expanded protections for undocumented and illegal immigrants (Trivett 2014).

Conclusions

While domestic terrorism in the United States was manifested in the name of various ideological agendas, since the beginning of the twenty-first century, the far right, Jihadi, and environmental associations dominate the violence. Moreover, while Jihadi violence is perpetrated mainly by inspired individuals, the American Far Right and the environmental movement consist today of multiple organizations with significant differences regarding their ideological origin, organizational structure, and preferred tactics.

Also, it seems that most domestic terrorism today is perpetrated by groups which are increasingly decentralized and thus provide more of a general ideological and logistical infrastructure rather than direct guidance for specific acts of political activism. It seems that the dramatic changes in modern communication technology also facilitated this process of decentralization, as it allowed ideological movements to establish virtual communities where members can pick and choose the type of ideas and activities they are interested in promoting.

Lastly, the growing political polarization in the American political system and populace may further incentivize and legitimize militant manifestation of political activism and thus provide greater operational space for domestic groups who are considering the use of violent tactics.

Cross-References

- ▶ Criminals: Terrorists
- ▶ Department of Homeland Security (DHS)
- ▶ Terrorism: Homegrown

References

Anti-Defamation League. (2005a, July 29, 2002). The Hammerskin Nation. Retrieved from http://archive.adl.org/learn/ext_us/hammerskin.html on 1 Jan 2017.

Anti-Defamation League. (2005b). Outlaw Hammerskins. Retrieved from http://archive.adl.org/learn/felton/hammerskins.html on 28 Nov 2016

Audsley, D. (1985). POSSE COMITATUS: An extremist tax protest group. *TVI Journal, 6*(1), 13–16.

Barkun, M. (1997). *Religion and the racist right: The origins of the Christian Identity Movement*. Chapel Hill: The University of North Carolina Press.

Belew, K. (2018). *Bring the war home: The white power movement and Paramilitary America*. Cambridge, MA: Harvard University Press.

Berger, J. M. (2016a). *The Turner legacy: The storied origins and enduring impact of White Nationalism's Deadly Bible* (24680656). Retrieved from

Berger, J. M. (2016b). *Without prejudice: What sovereign citizens believe*. Retrieved from Washington, DC. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Occasional%20Paper_Berger.pdf

Bjelopera, J. P. (2013). *The domestic terrorist threat: Background and issues for congress*. Washington, DC: Congressional Research Service.

Bjelopera, J. P. (2014). *The domestic terrorist threat: Background and issues for congress*. (7-5700). Washington, DC: Congressional Research Service.

Blee, K. (2002). *Inside organized racism: Women in the hate movement*. Berkeley: University of California Press.

Borum, R., & Tilby, C. (2005). Anarchist direct actions: A challenge for law enforcement. *Studies in Conflict and Terrorism, 28*(3), 201–223. https://doi.org/10.1080/10576100590928106.

Carson, J. V., LaFree, G., & Dugan, L. (2012). Terrorist and non-terrorist criminal attacks by radical environmental and animal rights groups in the United States, 1970–2007. *Terrorism and Political Violence, 24*(2), 295–319. https://doi.org/10.1080/09546553.2011.639416.

Colson, D. (2014). Erasing Anarchism: Sacco and Vanzetti and the logic of representation. *American Quarterly, 66*(4), 943–969. https://doi.org/10.1353/aq.2014.0073.

Craig, D. (2018, July 20). Bridesburg residents finding KKK recruitment materials distributed in their neighborhood. Retrieved from https://www.phillyvoice.com/bridesburg-residents-kkk-recruitment-flyers-philadelphia/ on 14 Aug 2018.

Dobratz, B. A., & Shanks-Meile, S. L. (1997). *"White power, white pride!": The white separatist movement in the United States*. New York City: Twayne Publishers.

Durham, M. (2000). *The Christian right, the far right and the boundaries of American conservatism*. Manchester: Manchester University Press.

Durham, M. (2003). The American far right and 9/11. *Terrorism and Political Violence, 15*(2), 96–111. https://doi.org/10.1080/09546550312331293057.

Federal Bureau of Investigation. (2010). *Domestic terrorism: The sovereign citizen movement*. Retrieved from Washington, DC. https://www.fbi.gov/news/stories/2010/april/sovereigncitizens_041310/domestic-terrorism-the-sovereign-citizen-movement.

Federal Bureau of Investigation. (n.d.). Terrorism. Retrieved from https://www.fbi.gov/investigate/terrorism on 8 Sept 2018.

Forest, J. J. F. (2012). *The terrorism lectures: A comprehensive collection for students of terrorism, counterterrorism, and national security.* Santa Ana: Nortia Press.

González-Cruz, M. (2008). Puerto Rican revolutionary nationalism. *Latin American Perspectives, 35*(6), 151–165. https://doi.org/10.1177/0094582x08326014.

Hafner, J. (2018, August 6). Ku Klux Klan Flyers left with candy in suspected effort to recruit children in New York. Retrieved from https://www.usatoday.com/story/news/nation-now/2018/08/06/klu-klux-klan-flyers-candy-found-children-upstate-new-york/919187002/ on 14 Aug 2018.

Levitas, D. (2002). *The terrorist next door: The militia movement and the radical right*. New York City: Thomas Dunne Books, St. Martin's Press.

Liddick, D. R. (2014). The radical environmental and animal liberation movements. In G. Michael (Ed.), *Extremism in America* (pp. 249–273). Gainsville: University Press of Florida.

MacDonald, A. (1978). *The turner diaries: A novel* (2nd ed.). Fort Lee: Barricade Books.

MacNab, J. J. (2017, February 14). Anti-government extremist violence and plots. Retrieved from http://www.seditionists.com/antigovviolence.pdf on 16 July 2017.

McVeigh, R. (2009). The rise of the Ku Klux Klan: Right-wing movements and national politics. Minneapolis: University of Minnesota Press.

McVeigh, R., Myers, D. J., & Sikkink, D. (2004). Corn, Klansmen, and Coolidge: Structure and framing in social movements. *Social Forces, 83*(2), 653–690.

Munson, Z. W. (2008). *The making of pro-life activists*. Chicago: The University of Chicago Press.

Nero, C. (2018, August 12). KKK recruitment flyers found in Suisun city neighborhoods. Retrieved from https://fox40.com/2018/08/12/kkk-recruitment-flyers-found-in-suisun-city-neighborhoods/ on 14 Aug 2018.

Noble, K. (2010). *Tabernacle of hate: Seduction into right-wing extremism*. Syracuse: Syracuse University Press.

Perliger, A. (2012). *Challengers from the sidelines: Understanding America's violent far-right*. Retrieved from The Combating Terrorism Center at West Point: https://ctc.usma.edu/challengers-from-the-sidelines-understanding-americas-violent-far-right/

Perliger, A. (2017a, October 18). Are many hate crimes really examples of domestic terrorism? Retrieved from https://theconversation.com/are-many-hate-crimes-really-examples-of-domestic-terrorism-85948 on 20 Oct 2017.

Perliger, A. (2017b, May 28). Charlottesville attack shows homegrown terror on the right is on the rise. Retrieved from https://theconversation.com/charlottesville-attack-shows-homegrown-terror-on-the-right-is-on-the-rise-78242 on 20 Oct 2017.

Pitcavage, M. (2001). Camouflage and conspiracy: The militia movement from Ruby Ridge to Y2K. *American Behavioral Scientist, 44*(6), 957–981.

Pollard, J. (2016). Skinhead culture: the ideologies, mythologies, religions and conspiracy theories of racist skinheads. *Patterns of Prejudice, 50*(4-5), 398–419. https://doi.org/10.1080/0031322x.2016.1243349.

Queally, J. (2016, February 29). Ku Klux Klan rally in Anaheim erupts in violence; 3 are stabbed and 13 arrested. Retrieved from http://www.latimes.com/local/lanow/la-me-ln-klan-rally-in-anaheim-erupts-in-violence-one-man-stabbed-20160227-story.html on 4 Oct 2018.

Rice, A. S. (1972). *Ku Klux Klan in American politics*. New York: Haskell House Publishers.

Seger, K. A. (2001). *Left-wing extremism: The current threat*. Retrieved from https://digital.library.unt.edu/ark:/67531/metadc724454/ on 26 Nov 2018.

Sharpe, T. T. (2000). The identity Christian Movement: Ideology of domestic terrorism. *Journal of Black Studies, 30*(4), 604–623.

Simi, P., & Futrell, R. (2010). *American swastika: Inside the white power movement's hidden spaces of hate*. Lanham: Rowman & Littlefield Publishers.

Southern Poverty Law Center. (2009). *The second wave: Return of the militias*. Retrieved from https://www.splcenter.org/20090731/second-wave-return-militias on November 26, 2018.

Southern Poverty Law Center. (2012). Racist skinheads: understanding the threat. *Intelligence Report*. Retrieved from https://www.splcenter.org/20120625/racist-skinheads-understanding-threat on 26 Nov, 2018.

Southern Poverty Law Center. (n.d.). National alliance. Retrieved from https://www.splcenter.org/fighting-hate/extremist-files/group/national-alliance on 28 Nov 2016.

Sullivan, B. A., Freilich, J. D., Chermak, S. M., Parkin, W., & Gruenewald, J. (2015). Financial crimes perpetrated by far-right extremists in the United States: 1990–2013 [Press release].

Sweeney, M. M., & Perliger, A. (2018). Explaining the spontaneous nature of far-right violence in the United States. *Perspectives on Terrorism*, 12(4).

Swenson, K. (2018, August 3). As far-right marchers and antifa prepare to face off on Saturday, Portland braces for violence. Retrieved from https://www.washingtonpost.com/news/morning-mix/wp/2018/08/03/as-far-right-marchers-and-antifa-prepare-to-face-off-on-saturday-portland-braces-for-violence/?utm_term=.08507e1a6c14 on 14 Aug 2018.

TOI Staff. (2017, January 10). FBI reopens case of 1973 assassination of Israeli diplomat. Retrieved from https://www.timesofisrael.com/fbi-reopens-case-of-1973-assassination-of-israeli-diplomat/ on 4 Oct 2018.

Trivett, D. W. (2014). The Chicano Separatist Movement. In G. Michael (Ed.), *Extremism in America* (pp. 114–146). Gainsville: University Press of Florida.

van Dyke, N., & Soule, S. A. (2002). Structural social change and the mobilizing effect of threat: Explaining levels of patriot and militia organizing in the United States. *Social Problems, 49*(4), 497–520.

Vertigans, S. (2007). Beyond the Fringe? Radicalisation within the American far-right. *Totalitarian Movements and Political Religions, 8*(3), 641–659. https://doi.org/10.1080/14690760701571254.

Wade, W. C. (1987). *Fiery cross: The Ku Klux Klan in America*. New York: Simon and Schuster.

Winter, A. (2014). Antiabortion extremism and violence in the United States. In G. Michael (Ed.), *Extremism in America* (pp. 218–248). Gainesville: University Press of Florida.

Further Reading

Michael, G. (Ed.). (2013). *Extremism in America*. Gainesville: University Press of Florida.

Terrorism: Homegrown

Christopher Cleary
St. John's University, New York, NY, USA

Keywords
Homegrown violent extremist · Foreign terror organization · Radicalization

Definition

Homegrown terrorism is acts of terrorism targeting the citizens, institutions, or government within the country in which the terrorist resides. Homegrown terrorism falls into two categories: *domestic terrorism* and *homegrown violent extremism (HVE)*.

- *Domestic terrorism* is acts of terrorism inspired by the US-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature. (Federal Bureau of Investigation, 2018)*
- *Homegrown violent extremist* (HVE) refers to a US-born or naturalized citizen who is inspired by the ideology of a foreign terror organization to commit acts of terrorism targeting the citizens, institutions, or government within the United States. Many HVEs act independently and do not receive any financial or operational support from the foreign terror organization (Bjelopera, 2018).

Foreign terror organization (FTO) is a label designated by the US Secretary of State to foreign organizations that engage in terrorist activity which threatens the security of US nationals or the national security of the United States (Department of State, 2018).

Left-wing terrorism involves acts of terrorism based on extreme interpretations of left-wing ideologies, including anti-capitalism, anti-imperialism, revolutionary communism or socialism, and anarchism. These ideologies are primarily revolutionary and use violence to eliminate what they believe to be social or class inequality.

Right-wing terrorism is acts of terrorism committed in support of extreme interpretations of right-wing ideologies, including racial supremacy, ethno-nationalism, and anti-government sentiment. Ethno-nationalist extremists employ a radical support for the political interests of a particular ethnic group.

Religiously motivated terrorism involves acts of terrorism based on the extreme interpretation of any religion or faith-based belief system. The terrorists justify the violence as being required by their religious dogma. There have been extremists in all major religions who have used violence in support of their radical religious beliefs.

Single-issue terrorism involves act of terrorism committed for a singular issue, including anti-abortion, animal rights, and environmental issues.

Introduction

Terrorism is a tactic which has been used throughout the world by individuals and groups willing to use violence and/or the threat of violence to create fear in a population for the purpose of causing political or social changes. There is no universally accepted definition of terrorism, but most definitions regard terrorism as an act that involves the threatened or actual use of ideologically motivated violence or illegal force used to accomplish political, social, or religious objectives.

Homegrown terrorism falls into two distinctly different categories: domestic terrorism and homegrown violent extremism. US law enforcement agencies categorize acts of domestic terrorism separately from attacks by homegrown violent extremists. Domestic terrorism is acts of terrorism inspired by US-based movements that espouse extremist ideologies of a political, religious, social, racial, or environmental nature (Federal Bureau of Investigation, 2018).

Homegrown violent extremism, in contrast, involves US-born citizens, naturalized citizens,

*Domestic terrorism is examined more fully in a separate section of this encyclopedia.

or citizens residing within the United States who are influenced to commit acts of terrorism by the extremist beliefs espoused by FTOs (Bjelopera 2018). A current example of a HVE in the United States is the religiously motivated threat from foreign terror organizations al-Qaeda and the Islamic State.

Homegrown Terrorism Ideologies

Throughout history, there have been notorious examples of individuals and groups engaging in unlawful acts of terrorism. Acts of terrorism are most often attributed to groups or individuals who espouse an ideology or belief system which they use to justify their actions. These ideologies can be described and categorized based on the nature of their extremist beliefs. Most frequently, they are labeled as right-wing, left-wing, religiously motivated, and single issue. These ideologies are extreme interpretations of legitimate, non-violent causes.

Right-wing extremist ideologies include racial supremacy, ethno-nationalism, and anti-government sentiment. In the United States, between 2007 and 2016, 74% of the 372 people killed by domestic extremists were killed by right-wing extremists (Anti-Defamation League 2016). According to Europol, the number of arrests for right-wing extremism in European countries rose from 12 in 2016 to 20 in 2017. It is believed that the recent rise in right-wing extremism was triggered by the influx of Muslim refugees and fear of the Islamization of Europe (Europol 2018).

Left-wing ideologies include anti-capitalism, anti-imperialism, revolutionary communism or socialism, and anarchism. The extremist interpretation of these ideologies advocates violence against government institutions or targets that represent capitalism. Between 1970 and 2016, 41 police officers in the United States have been killed by left-wing extremists (Anti-Defamation League 2016).

Religiously motivated terrorism based on the extreme interpretation of religious dogma has become a prominent threat against western societies. The terrorists justify their use of violence as being required to defend their religious beliefs. There have been extremists in all major religions who have used violence in support of their radical religious beliefs.

Single-issue terrorism committed by anti-abortionists, animal rights advocates, and environmental activists is unlike right-wing, left-wing, and religiously motivated terrorism because of its singular issue. These extremists are not seeking broader political or religious change. They only seek to cause changes to their primary cause.

The US Constitution protects American citizens' ability to seek out and adopt messages from individuals or groups that advocate terrorism, violence, or other unpopular ideologies. It is only when those citizens violate or attempt to violate state or federal laws in furtherance of those ideologies that their constitutional protection ends. American citizens are free to speak in favor of terrorist groups or agendas, but if they take action that violates the law, such as providing support to terror groups, committing crimes in furtherance of a terror organization, or recruiting others to do so, those citizens may be subject to prosecution (Federal Bureau of Investigation, 2011).

Radicalization to Terrorism

Radicalization happens when an individual accepts an ideology that advocates violence to cause societal change and then becomes motivated to commit violence (U.S. Department of Homeland Security 2016). The process of radicalization can begin through social or familial contacts who promote the extremist ideology or by self-radicalization. The ubiquitous nature of modern communications technology, the Internet, and social media facilitates self-radicalization. Individuals residing in the United States can now become fully immersed in conflicts and ideological causes occurring in foreign countries with no, or very little, censorship or delay in the message. Constant communications from foreign organizations reach susceptible individuals who may be enticed to join a cause that is unpopular in

United States (International Public Safety Association 2018).

The FTOs al-Qaeda in the Arabian Peninsula (AQAP) and the Islamic State in Iraq and the Levant (ISIL) have become particularly adept at producing jihadist messages that target American and European individuals who might be susceptible to radicalization. Social media outlets provide terror organizations and their supporters the ability to exchange extremist propaganda and rhetoric with a like-minded global audience. A recent study by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) shows that American Islamic extremists had a higher rate of Internet radicalization than right-wing or left-wing extremists (START 2017). Online jihadi videos such as those posted by American-born cleric Anwar al-Awlaki sought to motivate and inspire people to adopt al-Qaeda's radical extremist ideology. Al-Awlaki, who was targeted and killed by a US drone strike in 2011, is believed to have inspired several notorious terror events, such as the 2009 Fort Hood shooting, the 2009 Christmas Day bomb plot, and the 2013 Boston Marathon bombing (Shane 2015).

Online magazines, such as *Inspire* magazine produced by AQAP (Hunter & Heinke, 2011) and *Rumiyah* magazine produced by ISIL, are written in the English language and target individuals living in western countries. A typical edition of these magazines contains articles and photos that justify and advocate the commission of violence, assassinations, murder, and mass murder against anyone who does not share the group's extreme religious views. They contain detailed instructions on methods to construct weapons and tactical advice for the commission of atrocities. The pressure cooker bombs used in the 2013 Boston Marathon bombing were similar to designs found in an *Inspire* magazine article "How to Build a Bomb in the Kitchen of Your Mom." It is legal to download these online magazines in the United States, but other countries such as the United Kingdom and Australia have prosecuted individuals for possession of the jihadist material.

To develop an understanding of HVEs, researchers examine how and why people become terrorists and look for factors which may cause the transition from being a lawful citizen to one who engages in violent and criminal behavior in furtherance of a cause. Attacks have been perpetrated by individuals from a wide range of ethnic, social, educational, and economic backgrounds. There have been several studies that have examined the radicalization of recent HVEs, but these studies are usually hampered by limited data sets and restricted access to the actual perpetrator. Without access to the person who has become radicalized, researchers sometimes rely on indirect evidence to develop their theories. While there are several explanations of the process to radicalization, researchers have not found any conclusive single reason that would explain why individuals would embrace the narrative of a foreign terror movement and then willingly engage in the support of, or the commission of, violent terror activity (Borum, 2012).

Recent examples of religiously motivated HVEs in the United States have become radicalized only after they converted to a new religion. Colleen LaRose, who became known as "Jihad Jane," adopted the Islamic religion as an adult. She was born and raised in Michigan, but after her conversion to Islam, she became radicalized and used the Internet to recruit other people to wage violent jihad. LaRose participated in a plot to murder a Swedish artist who had drawn a representation of the Prophet Muhammad. LaRose was sentenced to 10 years in prison after pleading guilty to terror offenses in US federal court. (Federal Bureau of Investigation 2014).

Bryant Neal Vinas was born in New York to parents who emigrated from South America. He was raised as a Catholic, but he converted to Islam as an adult and began using the name Ibrahim. Vinas is believed to have radicalized after viewing jihadist material on the Internet. He traveled to Pakistan and attended a terrorist training program where he worked with al-Qaeda planners to develop a plot to bomb the Long Island Rail Road in New York. Arrested before he could carry out his attack, Vinas plead guilty to conspiracy to murder and other terrorism offenses (Federal Bureau of Investigation 2016).

Examples of Homegrown Violent Extremism

Following the terror attacks of September 11, 2001, the United States has seen an increase in incidents of religiously motivated homegrown violent extremism, specifically those inspired by the terror groups al-Qaeda, Islamic State, or their affiliates. Testifying before the Senate Homeland Security and Government Affairs Committee, FBI Deputy Assistant Director Nikki Floris stated that the FBI "views the Islamic State of Iraq and Syria (ISIS) and homegrown violent extremists as the main terrorism threats to the United States" (Federal Bureau of Investigation 2017, p. 1).

The following cases are examples of individuals who have committed acts of terrorism against targets in their native or adopted country and have been motivated by extremist ideology of a FTO and were exposed to radical beliefs or posted radical messages online:

New York City Vehicle Attack – On October 31, 2017, Sayfullo Saipov drove a rented truck onto a bike path and pedestrian walkway in New York City, intentionally killing 8 pedestrians and injuring 12 others. Saipov was a legal resident of the United States after he emigrated from Uzbekistan in 2010.

When the truck that Saipov used in the attack collided with a school bus, he exited the vehicle yelling "Allahu Akbar" while brandishing what appeared to be two handguns but were in fact pellet and paintball guns. New York Police Department officers at the scene shot Saipov and arrested him before he could continue his attack. Investigators recovered Saipov's cellphones which contained videos and images of Islamic State propaganda and also showed Internet searches of New York City and Halloween.

After his arrest, Saipov confessed to planning the attack for over 1 year and that he had been inspired to commit the terror attack by ISIS videos. His plan was to kill as many people as possible on the pedestrian walkway and then proceed to the vicinity of the Brooklyn Bridge to kill additional pedestrians. He explained that he intentionally chose to commit his attack on Halloween, believing there would be more pedestrians on the streets. Saipov also stated that he felt good about what he had done in the attack (U.S. Department of Justice 2017).

Saipov's terrorist attack closely mirrored instructions found in the November 2016 edition of the ISIS magazine *Rumiyah*, which contained an article called "Just Terror Tactics." The article provides detailed instructions for the planning and execution of terror attacks using a vehicle as a weapon to kill non-believers. The article also advocates that the attacker should exit the vehicle when it can no longer be driven and continue the attack with handheld weapons (U.S. Department of Justice 2017).

Westminster Attack – On March 22, 2017, British-born Khalid Masood drove a vehicle across Westminster Bridge in the direction of the Palace of Westminster in London. Masood drove the vehicle onto the pedestrian walkway, intentionally striking pedestrians. He then crashed his vehicle into the perimeter fence of the Palace of Westminster, which is the meeting place of the United Kingdom's Houses of Parliament (Hill, 2018). Masood exited his vehicle and fatally stabbed an unarmed police officer before he was shot by another armed officer. The attack killed 5 victims and injured 50. Khalid Masood was born Adrian Russell Elms but changed his name upon conversion to Islam. Investigators discovered that Masood had posted jihadi messages on social media but found no indication that he had any direct instructions from al-Qaeda or the Islamic State (Metropolitan Police 2017).

Pulse Nightclub Shooting – At approximately 2:00 a.m. on June 12, 2016, Omar Mateen entered the Pulse nightclub in Orlando, Florida, and began shooting at patrons. Between the time he began his murderous attack and the time when he was killed by responding police officers, he had killed 49 people and wounded 53. This was the most lethal mass shooting in US history at the time. While Mateen was inside the nightclub, he made

two calls to Orlando Police in which he identified himself as an Islamic soldier and repeatedly pledged allegiance to Abu Bakr al-Baghdadi, the leader of the Islamic State. Mateen also told the police that he had an explosive vest similar to those used in the Paris terror attack and that a vehicle outside the club had explosives that would kill the police. Neither statement about the explosives was true, and no explosives were found by responding officers.

Mateen was born in New York and then moved to Florida with his family when he was 5 years old. He attended primary and secondary school in Florida and had several reports of behavioral issues. After graduation from high school, Mateen received a degree from Indian River State College and was working for a private security company at the time of the shooting.

The FBI reported that Mateen became radicalized by watching online jihadi videos. Although the Islamic State of Iraq and Syria claimed responsibility for the attack, investigators found no indication that Mateen had any contact with, or direction from, a FTO (Washington Post, 2016).

San Bernardino Shooting – On December 2, 2015, Syed Farook and Tashfeen Malik, a married couple, conducted a mass shooting at the Inland Regional Center in San Bernardino, California.

Syed Farook was employed as a Health Inspector by the San Bernardino County Department of Public Health and was present at the Inland Regional Center for a combined training session and holiday party on the day of the attack. He left the training session early without explanation but left his backpack on the table. Approximately 30 min later, Farook and Malik returned to the building, armed with assault rifles and wearing tactical clothing and masks. They entered the room and began shooting. They fired over 100 rounds, killing 14 people and injuring 22 others before fleeing the scene in a rented SUV.

After the shooting, the pair drove the SUV throughout the San Bernardino area until they were spotted by police officers. Approximately 4 h after the initial shooting, the couple stopped their SUV and initiated a violent shootout with police officers. Both Farook and Malik were killed. A triggering device was found in the vehicle. Farook's backpack, which he left at the Inland Regional Center, contained a remotely controlled improvised explosive device, but it was rendered safe by the responding bomb squad (Department of Justice 2016).

The FBI reports that the couple had become radicalized for at least 3 years prior to the attack and spent over 1 year making financial and tactical preparations. Prior to the attack, Ms. Malik used Facebook to declare her allegiance to the Islamic State (Nagourney et al. 2015).

Fort Hood Shooting – On November 5, 2009, 12 US service members and 1 civilian employee were killed and 32 were wounded in a mass shooting at the military base at Fort Hood, Texas. The shooter, Nidal Hasan, was a psychiatrist and a Major in the United States Army.

Hasan was born in Virginia and attended Virginia Tech University. After graduating with an Engineering Degree, he joined the US Army. In 1997, he entered medical school at the Uniformed Services University of the Health Sciences. During his medical residency at Walter Reed Army Medical Center and at subsequent assignments, Hasan's colleagues and superiors were aware of his growing violent Islamic extremism, but a post-attack investigation by the FBI and the Department of Defense showed that no action was taken against Hasan despite his troubling behavior (U.S. Senate Report 2011).

The investigation of Hasan revealed that he had become radicalized gradually over a period of several years, but the radicalization escalated in the 2 years prior to the attack. In 2007, Hasan was scheduled to deliver a presentation on a healthcare topic to fellow officers. Hasan's presentation was stopped after 2 min because of protests from the audience. Instead of a healthcare topic, Hasan's presentation espoused radical Islamic views,

including defending Osama bin Laden, justifying suicide bombings, and blaming the United States for problems in the Middle East (U.S. Senate Report 2011). Hasan sent messages to al-Qaeda associate Anwar al-Awlaki using Awlaki's website and participated in an essay contest praising Awlaki's leadership (Poppe 2018).

While religiously motivated extremism has been the prominent threat to the United States over the past few decades, historic review of terrorism trends shows that the threat is constantly changing and adaptive. Therefore, the possibility exists that HVEs motivated by foreign ideologies other than religion could threaten the United States in the future.

Conclusion

Homegrown terrorism involves individuals committing acts of terrorism that target the citizens, institutions, or government of the country in which they reside. Homegrown terrorism generally falls into two categories: domestic terrorism, which is motivated by domestic issues, and homegrown violent extremism.

Homegrown violent extremists are individuals who live and operate in the United States and engage in, or attempt to engage in, illegal terrorist activities and are inspired by the ideology of a foreign terror organization. Many HVEs act independently and do not receive funding or operational direction from the FTO. HVEs are distinct from domestic terrorists in that they adopt the ideology of a FTO, while domestic terrorists adopt the ideology of US-based movements.

There has been an increase in cases of religiously motivated homegrown violent extremism since the terror attacks of September 11, 2001. Most of these cases involve individuals inspired by the infamous attacks against the United States and other western nations by the terror group al-Qaeda, the Islamic State, or their affiliates.

While religious extremism has recently been a prominent motivation of HVEs in the United States, historic review of terrorism trends shows that the threat is constantly changing and adaptive. Therefore, the likelihood exists that HVEs with ideologies other than religion will threaten the United States in the future.

Cross-References

- ▶ Terrorism: Domestic
- ▶ Terrorism: International

References

Anti-Defamation League. (2016). Murder and extremism in the United States in 2016- An anti-defamation league report. https://www.adl.org/resources/reports/murder-and-extremism-in-the-united-states-in-2016

Bjelopera, J. (2018). Sifting domestic terrorism from hate crime and homegrown violent extremism library of congress. Congressional Research Service. Retrieved from https://fas.org/sgp/crs/terror/IN10299.pdf

Borum, R. (2012). Radicalization into Violent Extremism I: A Review of Social Science Theories. Journal of Strategic Security 4(4):7–36. Retrieved from http://scholarcommons.usf.edu/jss/vol4/iss4/2

Europol. (2018). European Union Agency for Law Enforcement Cooperation 2018. European Union terrorism situation and trend report 2018. https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017

Federal Bureau of Investigation. (2011). Domestic terrorism: Focus on militia extremism. https://www.fbi.gov/news/stories/domestic-terrorism-focus-on-militia-extremism

Federal Bureau of Investigation. (2014). Federal Judge sentences 'Jihad Jane' to serve 10 years in prison for role in plot to commit murder overseas. https://archives.fbi.gov/archives/philadelphia/press-releases/2014/federal-judge-sentences-jihad-jane-to-serve-10-years-in-prison-for-role-in-plot-to-commit-murder-overseas

Federal Bureau of Investigation. (2016). Yemeni national pleads guilty to conspiring to kill U.S. soldiers in Afghanistan. https://www.justice.gov/usao-edny/pr/yemeni-national-pleads-guilty-conspiring-kill-us-soldiers-afghanistan

Federal Bureau of Investigation. (2017). Nikki Floris, Deputy Assistant Director, Statement before the Senate Homeland Security and Government Affairs Committee, Washington, DC. December 6, 2017. https://www.fbi.gov/news/testimony/adapting-to-defend-the-homeland-against-the-evolving-international-terrorist-threat

Federal Bureau of Investigation. (2018). Terrorism definitions. https://www.fbi.gov/investigate/terrorism#Terrorism-Definitions

Hill, M. (2018). The Westminster Bridge terrorist attack 22nd March 2017 operation classific a report on the use of terrorism legislation. https://www.gov.uk/government/publications/the-westminster-bridge-terrorist-attack

Hunter, R., & Heinke, D. (2011). Radicalization of Islamist terrorists in the Western World. https://leb.fbi.gov/articles/perspective/perspective-radicalization-of-islamist-terrorists-in-the-western-world

International Public Safety Association. (2018). Homegrown violent extremism; Background, radicalization, and countering violent extremism, HVE policy task force. https://www.joinipsa.org/resources/Documents/IPSA%20HVE%20Info%20Brief%20-%20Background%20Radicalization%20and%20CVE%20-%20Feb%202018.pdf

Metropolitan Police. (2017). Update: Westminster terror attack. March 27, 2017. http://news.met.police.uk/news/update-westminster-terror-attack-231086

Nagourney, A., Masood, S., & Schmidt, M. (2015). Killers were long radicalized, F.B.I. investigators say. *New York Times*. https://www.nytimes.com/2015/12/08/us/fbi-says-san-bernardino-assailants-were-radicalized.html

Poppe, K. (2018). Nidal Hasan- A case study in lone actor terrorism. GW Program on Extremism. Retrieved from https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Nidal%20Hasan.pdf

Shane, S. (2015). The lessons of Anwar al-Awlaki. *New York Times Magazine*. https://www.nytimes.com/2015/08/30/magazine/the-lessons-of-anwar-al-awlaki.html

START. (2017). Profiles of individual radicalization in the United States (PIRUS) National Consortium for the Study of Terrorism and Responses to Terrorism (START). http://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus

U.S. Department of Homeland Security. (2016). Department of homeland security strategy for countering violent extremism. October 28, 2016. Retrieved from https://www.dhs.gov/sites/default/files/publications/16_1028_S1_CVE_strategy_0.pdf

U.S. Department of Justice. (2016). A critical incident review of the San Bernardino public safety response to the December 2, 2015, terrorist shooting incident at the Inland Regional Center. https://www.justice.gov/usao-cdca/file/891996/download

U.S. Department of Justice. (2017). Sayfullo Saipov charged with terrorism and murder in aid of racketeering in connection with lower Manhattan truck attack, 11/21/17. https://www.justice.gov/opa/pr/sayfullo-saipov-charged-terrorism-and-murder-aid-racketeering-connection-lower-manhattan

U.S. Department of State. (2018). Foreign terrorist organizations. https://www.state.gov/j/ct/rls/other/des/123085.htm

U.S. Senate Committee on Homeland Security and Governmental Affairs. (2011). The U.S. Government's failure to prevent the fort hood attack. https://www.hsgac.senate.gov/imo/media/doc/Fort_Hood/FortHoodReport.pdf

Washington Post. (2016). Orlando gunman who pledged loyalty to ISIS was 'homegrown' extremist radicalized online, Obama says. https://www.washingtonpost.com/news/post-nation/wp/2016/06/13/police-orlando-gunman-was-cool-and-calm-during-hostage-standoff/?noredirect=on&utm_term=.d2da52f6d903

Further Reading

Executive Office of the President of the United States. (2016). Strategic implementation plan for empowering local partners to prevent violent extremism in the United States. https://www.dhs.gov/sites/default/files/publications/2016_strategic_implementation_plan_empowering_local_partners_prev.pdf

McCauley, C., & Moskalenko, S. (2017). Understanding political radicalization: The two-pyramids model. https://www.apa.org/pubs/journals/releases/amp-amp0000062.pdf

Pregulman, A., & Burke, E. (2012). *Homegrown terrorism*. Washington, DC: Center for Strategic and International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/120425_Pregulman_AQAMCaseStudy7_web.pdf

Terrorism: International

Jared R. Dmello[1] and Arie Perliger[2]
[1]Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA
[2]School of Criminology and Justice Studies, Center for Terrorism and Security Studies, University of Massachusetts Lowell, Lowell, MA, USA

Keywords

International terrorism · Terrorist tactics · Militancy · Radicalism · International relations

Definition

Premeditated, politically motivated violence perpetrated against noncombatant targets by individuals and/or groups inspired by, or associated with, designated foreign terrorist organizations or nations.

Introduction

Most terrorist groups that were active before WWII operated in a single country or region. However, with the proliferation of Left-Wing and Religious groups in subsequent decades, a growing number of terrorist organizations started to operate in multiple countries, thus forcing law enforcement and scholars to address and explore terrorism also in an international context. Title 22 of the United States Code, Section 2656(d), defines terrorism as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents," further providing that *international* terrorism is a "terrorism involving citizens or the territory of more than one country." For example, if the American Sovereign Citizens Movement attacked a mosque in Los Angeles, that would be classified as a domestic terrorist attack, whereas if members from the same group traveled to Saudi Arabia to attack a mosque in Riyadh, that would be considered by most law enforcement organizations and legal authorities as international terrorism. Academics, however, seem to be more skeptic about the distinctions between domestic and international terrorism. Many tend to point out that the increasingly globalized nature of many terrorist organizations and their cellular structure make it difficult to determine if acts or campaigns of terrorism are executed by domestic or international actors.

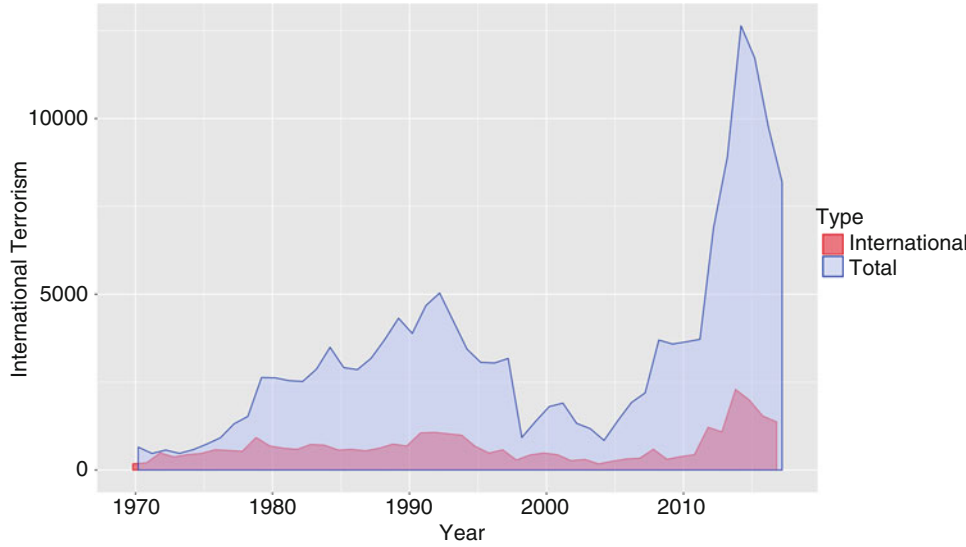
More specifically, while the statutory definition accounts for citizens and territories of multiple states, it fails to address cases in which militant ideology crosses state boundaries. For example, Alexander Blair and John T. Booker were American citizens charged with terrorist-related activity. After they were exposed to online propaganda of Jihadi groups, they posted statements online about their intent to wage jihad and their willingness to die for that cause. Based on the current legal statute, if these individuals were to conduct an attack within the United States, it would be an act of domestic terrorism, despite the influence of international Jihadi groups such as the Islamic State.

As these types of global trends become increasingly prevalent, it is clear that additional criteria need to be utilized in order to effectively distinguish between domestic and international terrorism. To this end, aspects from the Federal Bureau of Investigation's (n.d.) definition can be incorporated to produce a more comprehensive definition of international terrorism as *premeditated, politically motivated violence perpetrated against noncombatant targets by individuals and/or groups inspired by or associated with designated foreign terrorist organizations or nations*.

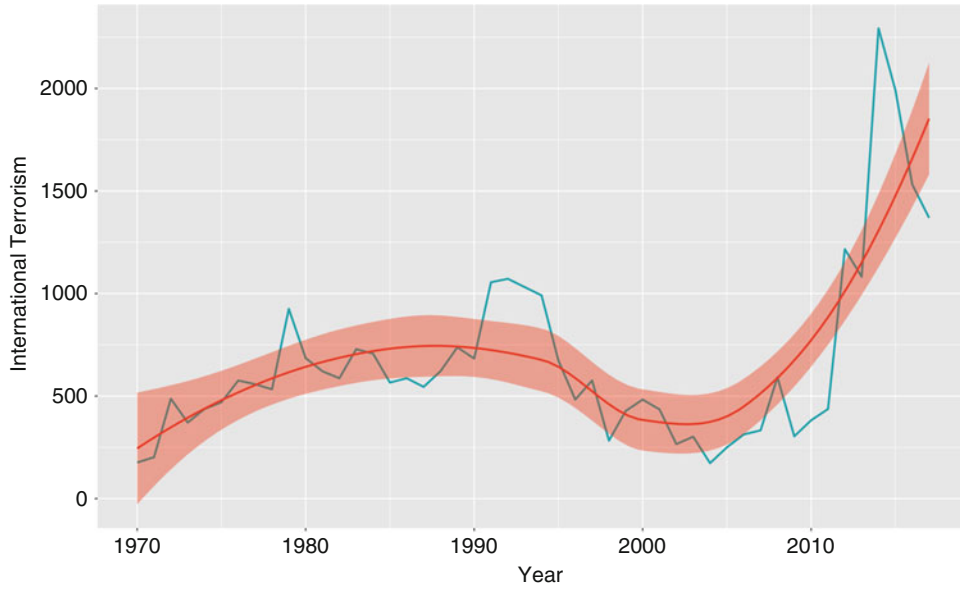
Trends

David Rapoport (2004) identified four historical waves of terrorism: (1) anarchist, (2) anticolonial, (3) leftist, and (4) religious. The first two ideological waves were inherently intrastate; the motivations for violence focus on specific geographic or political grievances (such as ethnic, separatist, or political slant). Left-wing terrorism, however, focused on the ideals of class struggle and individual empowerment within the framework of rejecting the nation-state model, concepts that transcend national boundaries. Both "class" and "religion," however, are social constructs, specific to certain times and geographic spaces. The power of religious fanaticism as a unifying cause for drawing support from a broader religious community has resulted in unprecedented levels of militancy (Ranstorp 1996); this can be seen through the activities of several international terrorist organizations, such as Al-Qa'ida and the Islamic State. Placed into context, in 2016, more countries than ever before experienced at least one death attributed to terrorism (Institute for Economics & Peace 2017).

Both international and domestic terrorism follow similar trends, as seen in Fig. 1: generally increasing from 1970 through 2017, with a brief period of decline during the 1990s. From roughly 2001 onward, terrorist activity has continued to increase at a rapid pace, with a global climax in 2014. International terrorist trends, in particular, have varied on a year-to-year basis, as shown in Fig. 2, but show a drastic increase coinciding



Terrorism: International, Fig. 1 Terrorist activity, total and international (1970–2017)

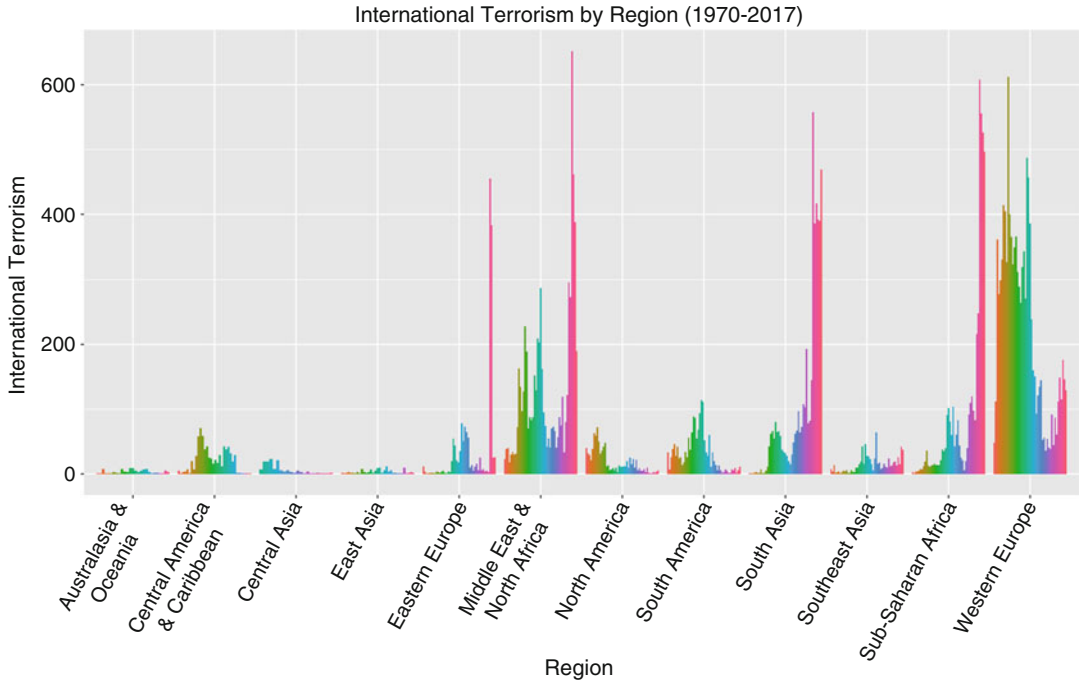


Terrorism: International, Fig. 2 International terrorism over time with mean slope (1970–2017)

with the proliferation of attacks by transnational extremist ideological actors such as Al-Qa'ida, the Islamic State, and their splinter organizations.

Geographical Focus

In the context of international terrorism, most experts identify the Middle East and North Africa as the regions which produced the highest number of attacks, as seen in Fig. 3. Moreover, many of the Middle Eastern groups also engaged in concentrated efforts to expand their operation into Western countries such as the United States and some of the dominant European nations (such as the UK, France, and Germany). Some of these



Terrorism: International, Fig. 3 International terrorism by region (1970–2017)

attacks were justified by militant religious convictions, while others were justified by the perceived Western exploitation of, and intervention in, countries in the region. The increasing capabilities of organizations such as Al-Qa'ida and the Islamic State further reflects that not as in the 1970s and 1980s, the proliferation of terrorism in the Middle East eventually impacted countries outside this region. Additionally, sustained military interventions in places such as Iraq, Afghanistan, and Lebanon also triggered retaliation in the form of international terrorism. For example, following the assassination of Abbas al-Musawi, the first leader of Hizbullah, by Israeli military forces, the organization retaliated by bombing and demolishing the Israeli embassy in Argentina and the Jewish community building in Buenos Aires, in 1992 and 1994, respectively. Similarly, the western coalition's military campaign in Iraq, which began in 2003, inspired retaliation by Western Jihadists, including the London 7/7 bombers.

The instability and internal conflicts in Afghanistan since the late 1970s, and the ongoing conflict between Pakistan and India, were some of the major factors which also led South Asia to experience exponential growth in the number of international terrorist incidents in the last few decades. For example, despite continued military intervention strategies from multiple countries, Pakistan's Federally Administered Tribal Areas (FATA) region remains a safe haven for transnational threats, such as Al-Qa'ida and the Taliban (Acharya et al. 2009; Gunaratna and Nielsen 2008; Rana 2009). Similarly, India has been plagued with terrorist-perpetrated violence. In 2008, Lashkar-e-Taiba, a Pakistan-based Islamic terrorist organization, engaged in a sustained shooting and bombing campaign at targets throughout the city of Mumbai, India. These individuals traveled to India specifically for the purpose of conducting this attack. While India did not take retaliatory military action against Pakistan, this situation further corroded trust between the two nations, impacting Indo-Pakistani relations (Javaid and Kamal 2013). Seven years earlier, Lashkar had engaged in an attack on the Indian Parliament in New Delhi in conjunction with Jaish-e-Mohammed, another Pakistan-based

group. This represents the spillover of diplomatic hostilities into asymmetric conflicts; India and Pakistan have historically had tense relations over multiple issues, most notably the disputed status of the accession of Jammu and Kashmir. Hence, Lashkar was a creation of the Pakistani Military Intelligence (ISI), which was looking in the late 1980s for ways to destabilize Kashmir, without being perceived as directly involved (Blank 2013).

Contradicting dynamics can be identified in other geographic regions, such as Central and East Asia, Australasia and Oceania, and Central America and the Caribbean. All these regions have actually seen decreases in victimization by international terrorism over time. It is not clear if this decline will persist, as some scholars argue that such dynamics may be cyclical. Feichtinger and Novak (2008), for example, assert that in the long run, government-terrorist dynamics remain in persistent oscillations, suggesting that a rise in terrorist activity in these areas may be on the horizon, as seen in areas like Eastern Europe and Southeast Asia where declines were followed by rising trends again.

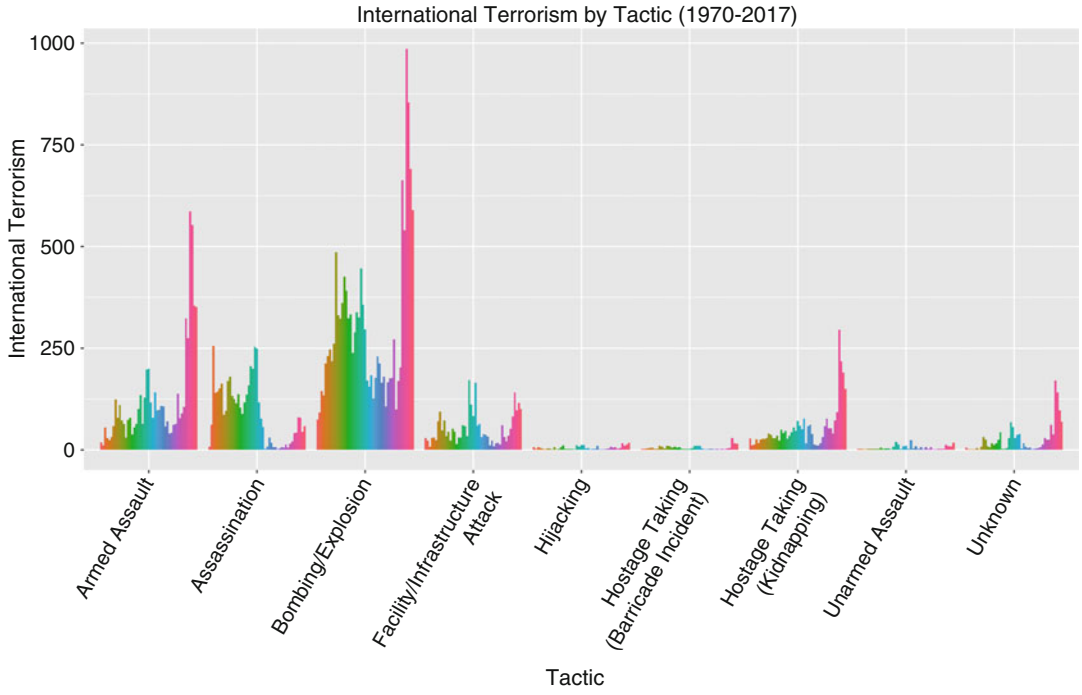
To conclude, international terrorism remains associated with weak and failed states (see Newman 2007). Contemporary examples include countries, such as South Sudan, Somalia, Libya, and Yemen (see Messner et al. 2018). Specifically, Piazza (2008) found that failed states are statistically more likely to (1) host international terrorist groups, (2) have their nationals commit international attacks, and (3) be targeted by international terrorists themselves. For example, Syria is a country engulfed in intrastate conflict. The Islamic State actively operates and engages in violence within Syria but also plans and perpetrates attacks globally. Beyond its own citizens joining these radical groups, individuals from around the planet have sought to travel to Syria to join ISIS (Binetti 2015; Franz 2015; Noonan and Khalil 2014; Patil and Ennis 2016).

Tactics

The tactics employed in campaigns of international terrorism vary broadly. However, a close examination reveals that some tactics experience a contingency effect and are quickly adopted by organizations if proven effective in previous or contemporary campaigns. The tactic of suicide bombing proliferated and was adopted by an array of organizations (such as LTTE and Hamas) after Hizbullah demonstrated its effectiveness in the early 1980s in its attacks in Lebanon (Pape 2003). Furthermore, Fig. 4, which provides insight into the usage of tactics by international terrorism over time, reflects crossover between tactics. For example, attacks involving targeting facilities and those with hostages often include overlap with other tactics.

Facility/Infrastructure Attacks are resurging, despite a previous decline. In 2009, Nidal Hasan fatally shot 13 people at Fort Hood in Texas, inspired by Jihadi Ideology Anwar al-Awlaki. One of the most common types of attacks is the targeting of Embassies and similar diplomatic and military facilities. In 2012, members of the Libya-based Ansar al-Sharia group attacked the United States Embassy in Benghazi, Libya, resulting in the death of the US ambassador and three other US citizens. Since the embassy itself is considered US territory, deaths occurring inside the embassy would be attributed to international terrorism. Similar attacks are the 1998 suicide attacks against the American embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, by Al-Qa'ida, as well as the attacks against the American embassies in Tehran and Islamabad in 1979. In both of the latter cases, radical college students stormed the US embassies taking diplomats as hostages (In Iran) or looking to harm the diplomatic personnel (as was the case in Islamabad when a Marine was killed) (Kohler 2000).

Hostage Taking was a popular tactic during the 1960s and the 1970s, especially in the context of aviation terrorism. Palestinian Nationalist and Left-Wing groups looking for attracting attention to their suffrage and goals mastered the practice of extending the attacks via hostage taking for days and weeks and maximizing the psychological impact and publicity they look to project. The kidnapping and killing of members of the Israeli delegation during the Munich Olympic games in 1972 by the Palestinian-based Black September organization is a case in point. While such kinds



Terrorism: International, Fig. 4 International terrorism by tactic (1970–2017)

of hostage-taking attacks are less popular today, many contemporary terrorist groups aim to kidnap specific individuals for ransom purposes or in order to attract attention to their ideological platform. In 2002, Daniel Pearl was abducted and eventually executed by the National Movement for the Restoration of Pakistani Sovereignty, after being deemed a "spy" of American interests (Musharraf 2006), an attack with lasting implications for US-Pakistani diplomatic relations. Similarly, in 2014, ISIS released videos showing the beheadings of two kidnapped American journalists, James Foley and Steven Sotloff, which prompted the Obama administration's declaration of retaliatory action against the Islamic State (Abdelaal et al. 2015).

Despite the evolution of military technology, *Bombings/Explosions* are still by far the most extensively employed tactics for engaging in terrorist activity. To execute these attacks, only rudimentary knowledge is necessary for bomb-making purposes, as well as basic know-how knowledge related to intelligence gathering and logistical practices. The proliferation of terror-produced magazines, such as Al-Qa'ida's *Inspire* and ISIS's *Dabiq*, and increasing access to the relevant operational information via online platforms have facilitated easier access to such knowledge (van Dongen 2016). For example, Dzhokhar Tsarnaev, one of the Boston Marathon bombers, learned how to weaponize pressure cookers from *Inspire*.

More capable organizations have utilized force multipliers in order to enhance the impact of this basic tactic, mainly via the use of suicide bombing and car bombs. The use of such force multipliers does not just help to maximize the damage of the attack but also serves an array of other objectives, such as illustrating the commitment of the organization to the cause, enhancing the symbolic and psychological impact of the violence, and allowing the organization to perpetrate more sophisticated operations. For example, within the radical jihadist movement specifically, suicide bombing has also been associated with martyrdom and the giving of one's entire self to the cause. This form of attack has been used in multiple contexts to build a symbolic narrative to political violence, an

idea that extends far beyond Islam (Khosrokhavar 2005). Research has found that the use of suicide campaigns overwhelmingly helps the terrorist organization's political cause (Pape 2003). The Tamil Tigers, a Sri Lankan-based organization, infamously integrated suicide campaigns into their operations, leveraging suicide campaigns as a source of symbolism to amass support for their cause (Roberts 2005).

Armed Assault is a commonly used terror tactic for extremist groups. This type of attack requires the least amount of planning and coordination while retaining the possibility to inflict high levels of damage. For example, in 2012, operatives of Al-Qa'ida in the Arabian Peninsula attacked an army base outside of Zinjibar city in Yemen, resulting in the deaths of 185 soldiers using firearms. Beyond global trends, Chasdi (2012) also found armed attacks to be the predominant tactic employed by terror organizations in both Algeria and Mali during the late 1990s. This tactic could be particularly appealing to organizations that lack the institutional capacity and resources needed for more coordinated operations or for individuals seeking to operate on behalf of a larger entity, such as assassinations of political leaders or bombings. For instance, in December 2015, 14 individuals were killed in a mass shooting "rampage" at a county-level government office in San Bernardino, California, by a married couple inspired by ISIS (Morell 2015). This example demonstrates the reach of some international groups, connecting with individuals not actually among their membership ranks (Johnson et al. 2016). For example, Koehler-Derrick and Milton (2017) argue that a group's strategic considerations and resource constraints explain tactic selection. Specifically, they find that groups with larger membership ranks are more likely to use firearms than their restricted counterparts because this tactic exposes the offender to higher levels of risk, such as apprehension or death, than other weapon choices.

The use of *assassinations* as a terrorist tactic has increased threefold from 1945–1969 to the 1970–2013 time period (Perliger 2015). The assassination of political leaders poses a direct challenge to the government's authority. Although this act could have a strong impact, drawing large amounts of attention to the organizational use while simultaneously causing a disruption in routine government operations, assassinations require higher levels of logistical planning than armed attacks. They tend also to intensify the prospects of a state's fragmentation and undermine the democratic infrastructure (Perliger 2015). Assassinations of diplomatic figures stationed abroad can be a mechanism for violent actors to send a powerful message to foreign powers from their own turfs. For example, in 1944, Lord Moyne, the UK's Minister Resident in the Middle East, was assassinated by two members of the Stern Gang or Lehi, a Zionist paramilitary organization focused on the end of British mandate in Palestine (Shpiro 2013). The assassination intensified British sentiments which called for the end of the UK rule of Palestine, a dynamic which eventually led to the end of the British rule in 1947.

Conclusion

While the majority of attention given to international terrorism by the media and political elite focuses on bombings in the Middle East or the Western World, political violence is a global epidemic that has transcended time, with groups employing a variety of tactics to achieve their strategic aims. Additionally, terrorists employ a wide array of tactics in their attacks. Each tactic requires different levels of organizational and tactical capacities, appeals to different types of actors, and impacts the intended targets differently.

Although "jihadism" is the current fascination of policymakers and researchers alike, transnational terrorist operations extend far beyond ideologies associated with radical elements of Islam. States with high levels of international conflict, such as Iraq and Syria (Carpenter 2013; Fearon 2007), alter the true nature of terrorist activity, since terrorism gets crossed with violence associated with the civil wars, providing a "white noise"

effect. The frequency of international terrorism is exponentially growing, increasing the urgency for the development and implementation of new counter-terrorism methods to address the growing threat.

Cross-References

- ▶ Criminals: Terrorists
- ▶ Investigations: Terrorism
- ▶ Terrorism: Domestic
- ▶ Terrorism: Homegrown

References

Abdelaal, N. M., Alisood, A. M., & Sase, A. S. (2015). Investigating Obama's ideology in his speech on Islamic State of Iraq and Levant (ISIL). *Journal of Applied Linguistics and Language Research, 2*(7), 228–246.

Acharya, A., Bukhari, S. A. A. S., & Sulayman, S. (2009). Making money in the mayhem: Funding Taliban insurrection in the tribal areas of Pakistan. *Studies in Conflict & Terrorism, 32*(2), 95–108.

Binetti, A. (2015). *A new frontier: Human trafficking and ISIS's recruitment of women from the West*. Information2Action: Georgetown Institute for Women, Peace & Security. http://giwps.georgetown.edu/wp-content/uploads/2017/10/Human-Trafficking-and-ISISs-Recruitment-of-Women-from-the-West.pdf

Blank, J. (2013). *Lashkar-e Taiba and the threat to the United States of a Mumbai-style attack*. Santa Monica: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/testimonies/CT300/CT390/RAND_CT390.pdf

Carpenter, T. G. (2013). Tangled web: The Syrian civil war and its implications. *Mediterranean Quarterly, 24*(1), 1–11.

Chasdi, R. J. (2012). Research note: Terrorism in Northwestern Africa: Mali, Mauritania, and Algeria: What START's quantitative data (1970–2011) can and cannot tell us. *Perspectives on Terrorism, 6*(2), 89–103.

Fearon, J. D. (2007). Iraq's civil war. *Foreign Affairs, 86*(2), 2–15.

Federal Bureau of Investigation. (n.d.). Terrorism. Retrieved from https://www.fbi.gov/investigate/terrorism. On 1 Oct 2018.

Feichtinger, G., & Novak, A. J. (2008). Terror and counterterror operations: Differential game with cyclical Nash solution. *Journal of Optimization Theory and Applications, 139*(3), 541–556.

Franz, B. (2015). Popjihadism: Why young European Muslims are joining the Islamic state. *Mediterranean Quarterly, 26*(2), 5–20.

Gunaratna, R., & Nielsen, A. (2008). Al Qaddafi in the tribal areas of Pakistan and beyond. *Studies in Conflict & Terrorism, 31*(9), 775–807.

Institute for Economics & Peace. (2017). *Global Terrorism Index 2017: Measuring and understanding the impact of terrorism*. New York: Institute for Economics & Peace.

Javaid, U., & Kamal, M. (2013). The Mumbai terror '2008' and its impact on the Indo-Pak relations. *South Asian Studies, 28*(1), 25–37.

Johnson, N. F., Zheng, M., Vorobyeva, Y., Gabriel, A., Qi, H., Velasquez, N., Manrique, P., Johnson, D., Restrepo, E., Song, C., & Wuchty, S. (2016). New online ecology of adversarial aggregates: ISIS and beyond. *Science, 352*(6292), 1459–1463.

Khosrokhavar, F. (2005). *Suicide bombers: Allah's new martyrs*. London: Pluto Press.

Koehler-Derrick, G., & Milton, D. J. (2017). Choose your weapon: The impact of strategic considerations and resource constraints on terrorist group weapon selection. *Terrorism and Political Violence*, 1–20. www.tandfonline.com/doi/abs/10.1080/09546553.2017.1293533

Kohler, M. (2000). To nations, a treaty, and the world court – An analysis of United States-Iranian relations under the Treaty of Amit before the International Court of Justice. *Wisconsin International Law Journal, 18*, 287.

Messner, J. J., Haken, N., Taft, P., Onyekwere, I., Blyth, H., Fiertz, C., Murphy, C., Quinn, A., & Horwitz, M. (2018). *Fragile States Index 2018*. Washington, DC: The Fund for Peace.

Morell, M. (2015). *The Great War of our time: The CIA's fight against terrorism – From Al Qa'ida to ISIS*. New York: Twelve.

Musharraf, P. (2006). *In the line of fire: A memoir*. New York: Simon and Schuster.

Newman, E. (2007). Weak states, state failure, and terrorism. *Terrorism and Political Violence, 19*(4), 463–488.

Noonan, M., & Khalil, P. (2014). North American foreign fighters. *Journal for Deradicalization, 1*, 66–96.

Pape, R. A. (2003). The strategic logic of suicide terrorism. *American Political Science Review, 97*(3), 343–361.

Patil, T., & Ennis, G. M. (2016). Silences as a discourse in the public sphere: Media representations of Australians joining the fight in Syria. *Social Alternatives, 35*(1), 6–12.

Perliger, A. (2015). *The rationale of political assassinations*. Retrieved from The Combating Terrorism Center at West Point. https://pdfs.semanticscholar.org/febe/e34d18053f78ae887f219366ecba6b7190d4.pdf

Piazza, J. A. (2008). Incubators of terror: Do failed and failing states promote transnational terrorism? *International Studies Quarterly, 52*(3), 469–488.

Rana, M. A. (2009). *Taliban insurgency in Pakistan: A counterinsurgency perspective*. Pakistani Institute for Peace Studies. https://www.pakpips.com/web/wp-content/uploads/2017/11/169.pdf
Ranstorp, M. (1996). Terrorism in the name of religion. *Journal of International Affairs, 50*(1), 41–62.
Rapoport, D. C. (2004). Four waves of modern terrorism. In A. K. Cronin & J. M. Ludes (Eds.), *Attacking terrorism: Elements of a grand strategy* (pp. 46–73). Washington, DC: Georgetown University Press.
Roberts, M. (2005). Tamil Tiger "martyrs": Regenerating divine potency? *Studies in Conflict and Terrorism, 28* (6), 493–514.
Shpiro, S. (2013). The intellectual foundations of Jewish national terrorism: Avraham Stern and the Lehi. *Terrorism and Political Violence, 25*(4), 606–620.
van Dongen, E. (2016). *A comparative content analysis of the extremist magazines 'Dabiq' (IS) and 'Inspire' (AQAP)*. Dissertation, Universiteit Leiden.

Further Reading

Caruso, R., & Schneider, F. (2011). The socio-economic determinants of terrorism and political violence in Western Europe (1994–2007). *European Journal of Political Economy, 27*, S37–S49.
Cronin, A. K. (2003). Behind the curve: Globalization and international terrorism. *International Security, 27*(3), 30–58.
Dale, S. F. (1988). Religious suicide in Islamic Asia: anti-colonial terrorism in India, Indonesia, and the Philippines. *Journal of Conflict Resolution, 32*(1), 37–59.
Forest, J. (2012). The terrorism lectures: A comprehensive collection for students of terrorism, counterterrorism, and national security. Nortia Press.
Gaibulloev, K., & Sandler, T. (2008). Growth consequences of terrorism in Western Europe. *Kyklos, 61*(3), 411–424.
Gause III, F. G. (2005). Can democracy stop terrorism? Foreign Affairs, 62–76.
Jenkins, B. M. (1985). International terrorism: The other world war (No. RAND/R-3302-AF). RAND CORP SANTA MONICA CA.
Jenkins, B. M. (2015). International terrorism: A new mode of conflict. In International terrorism and world security (pp. 23–59). Routledge
LaFree, G., & Dugan, L. (2007). Introducing the global terrorism database. *Terrorism & Political Violence, 19*(2), 181–204.
Midlarsky, M. I., Crenshaw, M., & Yoshida, F. (1980). Why violence spreads: The contagion of international terrorism. *International Studies Quarterly, 24*(2), 262–298.
Pedahzur, A. (Ed.). (2006). Root causes of suicide terrorism: The globalization of martyrdom. Routledge.
Perliger, A. (2012). How Democracies Respond to Terrorism: Regime Characteristics, Symbolic Power and Counterterrorism. *Security Studies, 21*(3), 490–528.
Piazza, J. A. (2008). A supply-side view of suicide terrorism: A cross-national study. *The Journal of Politics, 70*(1), 28–39.

Tort: Property

Adam Scott Wandt
John Jay College of Criminal Justice, New York, NY, USA

Keywords
Tort · Trespass · Conversion · Nuisance · Easements

Definition

1. An unlawful interference by a tortfeasor with the enjoyment of another's private property.
2. A subcategory of torts, relating to damaged property.

Introduction

Damage and interference with land and property is inevitable as members of society regularly interact with one another in public and private forums. We rely on our civil legal system to make victims financially whole through remedies and to influence the way people operate in society (i.e., to be more careful).

This damage and interference may involve another person's real property (i.e., land) or personal property (known as "chattel"). Tort law provides the loss allocation function of defining the conditions under which, and the extent to which, a tortfeasor (i.e., a person who commits a tort) has to compensate an injured party. The law prescribes very specific guidelines for courts to award damages to injured parties. Tort law seeks to aid in the prevention and mitigation of future damage; since remedies are readily available to an injured party, it is hoped that the threat of sanctions will deter a possible tortfeasor from causing damage.

In this entry we will explore the tort of nuisance, trespass to real property, the concept of easements, the doctrine of trespass ab initio, trespass to chattels, defenses to trespass, and the tort of conversion.

A Short History of Property Tort Law

It is believed that the Code of Hammurabi (c. 1754 BCE) (the "Code") is the oldest surviving legal writings of significant length and substance that deal with tort law. The Code is one of the earliest examples of a presumption of innocence and is seen as an early example of fundamental law that regulated ancient society. The Code allows an injured party to respond to a tortfeasor by inflicting a similar type of damage ("an eye for eye, and a tooth for a tooth"). The Code includes remedies for those injured by a negligent builder of a structure that collapses and for one's personal property that is damaged while in the care of a third party. Remedies for torts eventually matured with the introduction of the Roman's Lex Aquilia (c. 286 BCE), the first set of laws that promoted financial compensation of an injured party.

The development of liability for trespass evolved further under the English common law system. Absolute liability (liability regardless of deliberate intent, guilty mind, or harmful acts) was established in *Case of the Thorns* (England, 1466). In that case, a man cut his thorn bush and the thorns fell on his neighbor's lawn. The man walked onto his neighbor's land to retrieve the cut thorns and was held liable for trespass. This case established two important modern concepts: (1) that of absolute liability (i.e., the simple act of entering onto another person's property without authorization constitutes trespass) and (2) that ownership of land entitles an owner to exclude others.

English common law continued to hold that intent is not required for trespass. In *Weaver v. Ward* (England, 1616), the plaintiff and defendant were trained soldiers taking part in a military drill. The defendant accidentally, and against his will, discharged his musket and injured the plaintiff. The court awarded the plaintiff damages, holding that trespass does *not* require intent.

These early systems of law, such as the Code of Hammurabi and Lex Aquila, with influences from other cultures and societies, eventually developed into the English common law and French civil legal systems, which are commonly present throughout the legal world today.

Nuisance

Property owners are entitled to the quiet use and enjoyment of their land. A nuisance occurs when someone interferes with that use and enjoyment, whether through excessive noise, smells, pollution, or other hazard. It may occur during the unreasonable use of one's own property, so that it substantially impairs the rights of another to enjoy their own property. A nuisance is not just the "wrongful invasion of the use and enjoyment of property, but also the wrongful invasion of personal legal rights and privileges generally" (*Taylor v. Cincinnati,* 143 Ohio St. 426 (1944)).

The offensive conduct itself is not the nuisance, but the damage or consequences of the offensive conduct. The condition that creates a nuisance may create a danger to a person, property, or the public welfare.

Nuisance is different than trespass in that a trespass interferes with the rightful possession of property, whereas a nuisance interferes with the use and enjoyment of the property.

A nuisance can be (1) per se or at law or (2) per accidens *or in facts*. "A nuisance per se is an act, occupation, or structure that, by its very nature, is a nuisance at all times and under all circumstances" (*Morgan v. High Penn Oil Co, 238 N.C. 185* (1953)). A lawful act can never be nuisance per se. A nuisance per se can be prevented via legal action at all times. A nuisance per accidens is an act, occupation, or structure that becomes a nuisance by (1) reason of circumstance, location, or surroundings or by (2) the manner it is constructed, maintained, or operated (*Morgan v. High Penn Oil Co, 238 N.C. 185* (1953)).

A nuisance can be (1) private; (2) public; or (3) mixed. A private nuisance is non-trespassory "conduct that interferes with an individual's private right to the use and enjoyment of his or her land" (*Pestey v. Cushman*, 259 Conn. 345, 788 A.2d 496 (Conn. 2002)). Its roots are in property law. A public nuisance is an "unreasonable interference with a right common to the general public" (Rest. 2d). It traditionally interferes with a public right, public health, or public safety. Its roots are in criminal law, and thus claims for

public nuisance are generally brought by governmental units on behalf of the public. An individual may have standing to bring a civil claim for public nuisance if (s)he can show special injury (i.e., harm different from the kind suffered by others exercising the common right, such as physical injury) (*Philadelphia Electric Co. v. Hercules, Inc.* (1985, 3rd Cir)).

An example of a private nuisance is when a person plays loud music late into the evening and keeps his neighbor awake. An example of a public nuisance is a person keeping a very large number of domestic cats on their property or a cattle feedlot that emits noises and odors that waft onto nearby properties and are so strong that landowners are forced inside their houses.

Trespass to Land (Real Property)

The tort of Trespass to Land (i.e., real property) is any unauthorized intentional presence on one's land, or the illegal interference with one's lawful and productive use.

The Restatement of Torts (Second) prescribes:

> One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally (a) enters land in the possession of the other, or causes a thing or a third person to do so, or (b) remains on the land, or (c) fails to remove from the land a thing which he is under a duty to remove. (*Restatement of the Law (Second), Torts §158*)

A trespass may be committed on or above the surface of an owner's property. For example, the simple act of walking across a neighbor's lawn without permission is trespass, as is trespass to the air above another's land. In *Herrin v. Sutherland* (1925, MT), a duck hunter shot a gun over another's land and was held liable for trespass. However, for one to be liable for trespass beneath the surface of the land, such as with mining, actual damage is required for liability (i.e., absolute liability does *not* apply).

A trespass can be momentary, continuous, or permanent. For example, a momentary trespass occurs if a lost hiker wanders onto one's property for a few minutes without the owner's permission. A continuing trespass occurs if a person leaves an object or structure on another person's land without the owner's permission, even if the person initially had consent to be on the land (*Rogers v. Board of Road Commissioners for Kenty County* (1947)). To be considered a continuing trespass, the situation must be able to be remedied by restoring the land to its original state (otherwise it would be a permanent trespass). For example, a tortfeasor who plants a banana tree on his or her neighbor's land without permission is liable for continuing trespass the entire time the banana tree remains on the land, even if the original tortfeasor never returns (*Thorton v. Schiavello*, 93 A.3d 656 (2014)). A trespass becomes permanent when the land is distorted or changed in a way that cannot be undone and is indefinite. Permanent trespass becomes possible in situations where water is diverted or dirt is removed. For example, a tortfeasor may create a permanent trespass when (s)he wrongfully and permanently diverts a natural creek away from an owner's property, destroying the soil and vegetation.

Trespass to Land is known as an intentional tort, meaning liability attaches if a person's *actions* have the purpose or substantial certainty of producing the result. This means that liability attaches if one's *actions* that led to the trespass were intentional, or if one's *actions* had the substantial certainty to lead to trespass. In other words, the trespass itself does not have to be intentional. It also means that one may be held liable for trespass even though there is no injury to the land or interest of the owner (i.e., damages do not need to be proven). In cases where the trespass was reckless, negligent, or the result of an abnormally dangerous activity, trespass only attaches if the person's or object's presence causes harm to the land, owner, or third party with a protected right.

In most jurisdictions in the United States, "no trespass" signs are not required to enforce civil trespass, even where local laws require "no trespass" signs be posted for the enforcement of criminal trespass.

The duty owed to protect a trespasser varies state by state. In Keegan v. Lemieux Security

Services Inc., a college security officer was patrolling Middlebury College in Vermont when she observed men entering a dangerous construction site on campus. The college had contracted with the construction agent to provide fencing and dedicated security services for the site due to the inherent construction dangers present. Although the site was within the college boarders, campus security was not responsible for patrolling it. College Security Officer Keegan entered the construction site to pursue a trespasser and was injured during the apprehension. In the state of Vermont, "a landowner or occupier generally owes no duty of care to a trespasser, except to avoid willful or wanton misconduct." Keegan sued the construction agent and its security service for negligence, claiming they owed a duty to protect her from injury. The Supreme Court of Vermont affirmed the trial court's decision dismissing the claim holding that "the defendants owed no greater duty to the officer than they owed to trespasser, and thus officer failed to show that defendants breached a duty owed to her, precluding recovery on a negligence claim" (*Keegan v. Lemieux Security Services, Inc.*, 177 Vt. 575, 861 A.2d 1135, (Vt. 2004)).

A tortfeasor's subjective reasoning for being on the trespassed property, adherence to good faith, and ignorance as to his/her current location ("mistake of fact") are not acceptable defenses to civil trespass. Many jurisdictions recognize "necessity" as a defense to trespass. Necessity allows someone to enter and remain on someone's land in an emergency situation in order to prevent hardship. For example, necessity allows someone to take emergency shelter from a storm without the fear of liability for trespass. (Necessity and emergency are a type of consent – see section VI on Defenses below.)

In Lebovitz v. Sheraton Operating Corporation, the plaintiff was physically removed from a hotel for alleged trespass after refusing to leave upon being asked to by hotel security. Plaintiff alleged he agreed to leave, but only after talking to a hotel manager. Without being allowed to talk to the manager, the plaintiff alleged he was physically dragged from the hotel and turned over to New Orleans Police where he was arrested and charged with criminal trespass. Hotel security claimed to police that he was removed from the hotel for ticket scalping, something the plaintiff denied. The hotel's motion for Summary Judgement was denied by both the trial court and the Court of Appeals of Louisiana, holding that "Even if the statute gives the hotel authority to ask persons to leave, it does not give it the authority to make false statements to the police leading to the persons' arrest" (*Lebovitz v. Sheraton Oper.*, 868 So. 2d 164 (La. Ct. App. 2004)).

Civil damages and legal remedies available for trespass to land include:

1. Nominal damages, i.e., a minimal amount of money is rewarded mainly to recognize that the plaintiff was wronged.
2. Compensatory damages to compensate the plaintiff for his/her injury and to make him/her whole. This includes actual damages, i.e., the actual monetary value of the damage, to compensate the plaintiff for damage to land or personal property that occurred during the trespass.
3. Putative damages, for which the sole purpose is to punish the trespasser.
4. Injunctive relief, being a stop order from the court, to prevent certain future conduct.

Easements

An action for trespass may not be maintained where the accused has an easement. An easement is the irrevocable right to use another's land for a specific purpose. In other words, easements allow for a person to go onto the land of another and make limited use of that property, such as for ingress or egress. There are two types of easements.

First is an easement appurtenant, which requires two parcels of land, usually adjoining. For example, a property owner who owns landlocked property (the dominant tenement) without access to any public roads may have an automatic easement allowing for him/her to travel over a neighbor's land (the servient tenement) to access his/her property. The dominant tenant has the right to enter onto the land of the servient tenant; the servient tenant is burdened by/subject to the easement. These easements may be automatic or

agreed upon by two individuals. These easements most often "run with the land," meaning they pass with the title to real property and cannot be revoked due to sale or rezoning of the property. However, if such an easement is no longer needed due to a change in the physical land (e.g., if a new road is built allowing access to the landlocked property), that easement can be vacated and no longer valid. Landowners that violate another's right to an easement may be liable for damages. For example, a landowner may not build a fence or a structure on his or her own property if it would interfere with a preexisting easement. In addition, a third party may not take advantage of an easement that (s)he is not part of.

The second type of easement is an easement in gross, involving one parcel of land and one servient tenement that is subject to the easement. For example, municipalities have the right to install a sewer line across a property's owner land to connect the house to the sewer system, and municipalities have the right to install telephone polls on one's front lawn. These easements are "personal" in nature and are intended to benefit the holder personally rather than a connection with any land that the owner may hold. Such an easement usually gives the easement holder a right to do something on another's land.

Interfering with a person's lawful easement over real property is not allowed, and a damaged party has several civil remedies at their disposal including asking the court for an injunction to stop the interference, bringing an action for nuisance or another tort, or damages if there is a loss.

Trespass Ab Initio

The doctrine of trespass ab initio is when one enters legally upon land in the exercise of a privilege properly conferred and subsequently abuses the privilege by a trespass to person, chattels, or land. The tortfeasor becomes liable not only for the later misconduct but also forfeits the original lawful entry to become a trespasser "ab initio" or from the beginning (75 Am Jur 2d Trespass §51).

When a property owner gives permission for someone to enter his or her land for business or commercial purposes, the property owner issues a license for the visitor to be on the property; the property owner is the "licensor" and the visitor is the "licensee." The license can be revoked or expire if the visitor remains on the land past the stated purpose (*State v. Zembreski*, 445 N.J. Super. 412 (2016)).

Those who visit another's land for personal reasons are classified by law as "invitees." An invitee who remains on the property to use it in the scope of his or her own interest and not for the purposes invited loses his or her status as an invitee and automatically becomes a trespasser (*State v. Girardier*, 484 S.W.3d 356 (2015)).

A licensee or invitee that properly enters land and commits a tortious act thereafter is responsible only for the tortious act and not trespass ab initio. However, if the entry to the land was fraudulent and only for the purpose of committing a tortious act, the tortfeasor can be held liable. Furthermore, in the event a licensee exceeds the authorized access granted in the license, does not conform with the license terms, or is otherwise revoked, the acts committed in excess of the licensee's authority may constitute trespass ab initio (*State v. Girardier*, 484 S.W.3d 356 (2015)).

Illustrative Example 1: Ashley the Assaulter is out with friends at a local movie theater. Ashley and her friends properly purchased tickets from the theater giving them the status of licensee. While waiting for the movie to start, Ashley observes an old rival, Victoria, walking into the theater. Ashley approaches and assaults Victoria during the opening credits. Since Ashley was at the theatre legally and with legitimate intent, Ashley is most likely not liable for trespass ab initio.

Illustrative Example 2: Ashley the Assaulter is angry at Victoria and wishes to find and harm her. Ashley is out driving around looking for Victoria when she hears from a friend that Victoria is at a local movie theater. Ashley buys a movie ticket for the sole purpose of going into the theater and assaulting Victoria, a plan she then carries out. Ashley is most likely liable for trespass ab initio for gaining access to the movie theater by purchasing a ticket and becoming a licensee, with fraudulent intent.

Security personnel and private investigators looking to gain access to another's land should be careful not to use depict or they risk accidently committing the tort of trespass ab initio.

Trespass to Chattel

The Restatement of Torts (Second) explains that a trespass to chattel (i.e., personal property) lies in interference to the rightful possession or enjoyment of its owner. A trespass to chattel is the intentional use of or interference with personal property, which is in the possession of another, without justification. It can occur when one dispossesses another of the chattel; "the chattel is impaired as to its condition, quality, or value; the possessor is deprived of the use of the chattel for a substantial time; bodily harm is caused to the possessor; or harm is caused to some person or thing in which the possessor has a legally protected interest" (*Restatement of the Law (Second), Torts §218*).

Trespass to chattels arises where a tortfeasor's actions or interference with another's chattels falls short of that required for a conversion. Some jurisdictions differentiate between Trespass to Chattel and Conversion based on the amount of damage done or whether a replacement chattel is required.

Defenses to Trespass

Defenses to trespass, of significance, include the following:

Infancy: Infancy (being under the age of majority) is not a defense to liability in trespass, although infancy may prohibit someone from being able to form the necessary intent to commit trespass.

Consent: In some jurisdictions, the plaintiff must prove a lack of consent. Consent need not be verbal; it can be contextual and determined through context. Local customs and rules can help determine consent. Emergencies or necessities can create consent (as noted above).

Reclaiming Chattel: In some cases, actors may be privileged to enter onto another's land to reclaim a chattel that was left behind. This may include a child, pet, or other chattel that has wandered onto the land of another. For example, some jurisdictions would support a person entering another's property to retrieve a hat that was blown off one's head by the wind.

Authority of Law: The law sometimes prescribes privilege as a matter of law for specific individuals to be able to access property under certain circumstances. This type of privilege often extends to utility workers and other government officials who may need access to property in emergency situations.

Public Access to Waterways: Most jurisdictions in the United States recognize public access to the inter-tidal zone of a beach or costal waterway. This allows people to walk along the water's edge regardless of who owns the adjacent property.

Private Nuisance: In some jurisdictions a landowner may enter an adjoining property without permission for the purpose of abating a condition that affects his/her land that constitutes a nuisance to the possessor's interest. A common example would be where landowner X does not visit his or her property often and a barn on X's property is broken into and used by local teenagers to host parties. X's neighbor is within his or her rights to enter onto X's property to board up the barn, preventing the teenagers from entering in the future. Examples of other types of supported abatement include trash removal and removal of a damaged tree.

Public Nuisance: A public safety officer may enter another's land, at a reasonable time and in a reasonable manner, for the purposes of abating a public nuisance (§ 202 Abatement of Public Nuisance by Public Official. Restat 2d of Torts, § 202).

Arrests: Government officials with arrest power for criminal offenses carry the privilege to enter another's land for the purpose of making an arrest.

Statute of Limitations: A statute of limitations is legislation that establishes the maximum time in which plaintiffs can bring an action after a tort or other offense has been committed. In most cases, the law prevents an injured party from taking legal action after a certain number of years after the

injury occurs or is discovered. Different civil wrongs have different prescribed time limitations. Not taking action on a permanent trespass, past the statute of limitations, may leave no possible remedies for the plaintiff.

Conversion

The Restatement of Torts (Second) defines conversion as an "intentional exercise of dominion or control over a chattel (personal property) of another, which so seriously interferes with the right of another to control it that the tortfeasor may justly be required to pay the owner the full value of the chattel" (*Restatement of the Law (Second), Torts §229*). As an "intentional tort," like trespass, only the tortfeasor's intent to control the chattel is necessary to find liability; the tortfeasor is not required to have the intent to dispossess the true owner of the chattel or even to know that the object belongs to another.

Today, English-speaking society colloquially refers to the tort of conversion as "theft." While there are some differences in the elements and relative intent, conversion is to civil law what theft/larceny is in criminal law. Theft/larceny is a criminal offense that is prosecuted by the state; conversion is a civil offense, where a complaint is brought forward in civil court by an injured party (the plaintiff).

Actions for conversion generally lie with respect to chattels; real property (i.e., real estate) is not subject to conversion.

In order for a plaintiff to successfully establish a claim for conversion, the following elements must be met: (1) the plaintiff had legal title to the converted property; (2) the plaintiff either had possession of the property or the right to possess it at the time of the conversion; (3) the defendant exercised dominion over the property in a manner which denied the plaintiff his/her rights to use and enjoy the property; (4) in those cases where the defendant lawfully, or at least without fault, obtained possession of the property, the plaintiff made some demand for the property's return which the defendant refused; and (5) the plaintiff has suffered damage by the loss of the property (*McTiernan v. Jellis*, 2013 WY 151, 316 P.3d 1153, 2013; Gould *v. Ochsner*, 2015 WY 101, 354 P.3d 965 (Wyo. 2015)).

A tortfeasor's intent or motives are irrelevant in determining liability for conversion, but may be relevant in determining damages (*Taylor v. Forte Hotels Int'l*, 235 Cal. App. 3d 1119 (1991)). In other words, it does not matter why someone converted the chattel in determining his or her guilt, but his or her intentions may mitigate or compound how much money he or she has to pay the plaintiff in damages. It is also important to point out that conversion does not require the tortfeasor to have exclusive control of the converted chattel (*Quantlab Techs. Ltd. v. Godlevsky*, 719 F. Supp. 2d 766 (2010)). This means that a chattel can be converted that is still in the possession of its owner, so long as the owner can no longer use the item for its intended purpose. An unauthorized use of an umbrella, later followed by a return of a broken umbrella (non-intentional), leaves the owner wet and unable to enjoy the benefit of his chattel. Similarly, a tortfeasor can be held liable for conversion for intentionally destroying or materially altering a chattel.

Even where someone has been given limited rights to use a chattel, a tortfeasor can be held liable for conversion for exceeding authorized use of a chattel if the rights of another who has the right to control the chattel are violated.

A chattel does not have to have monetary value for a plaintiff to sustain an action of conversion (*Palm Beach Golf Center-Boca, Inc. v. John G. Sarris*, D.D.S., P.A., 771 F.3d 1274 (2014)). Conversion can be attached to include documents "that embody an intangible right, such as stock certificates and bonds" (*Iglesias v. United States*, 848 F.2d 362 (1988)). However, an action for conversion cannot lie in a standard unpaid debt (*Geler v. National Westminster Bank,* 770 F. Supp. 210 (1991)) or "where damages are merely being sought for breach of contract" (*Peters Griffin Woodward, Inc. v. WCSC, Inc.*, 88 A.D.2d 883, 452 N.Y.S.2d 599 (1982)).

Intellectual property such as poems and songs cannot be the subject of an action for conversion, unless they were reduced to a physical form and that physical form was converted (*Quantlab*

Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766 (2010)). Therefore, it would not be conversion to hand copy a written work onto a medium that one already owns. However, it would be conversion to use someone else's parchment to handwrite a poem.

Conversion deprives the rightful owner or user of the property permanently or for an indefinite time. Depriving an owner or user of his or her property for a short, finite time with the intention to return the property may not qualify as conversion (*Macomber v. Travelers Prop. & Cas. Corp.*, 261 Conn. 620 (2002)) (although it may qualify as trespass to chattels; see above). In cases where the defendant first legally borrowed the chattel in question, the plaintiff must make a demand for the property's return, with a refusal to deliver, before liability for conversion attaches. In many jurisdictions, this is true even where the borrower retains the chattel past an agreed-upon return date.

Illustrative Example 1: Boris the Borrower "borrows" his neighbor's lawn mower for 5 weeks straight; Boris took the lawn mower from his neighbor's shed without permission. Boris returns the lawn mower in the same condition he found it, with a full tank of fuel, and before the owner attempted to use it or noticed it missing. Boris the Borrower is most likely not liable for conversion. Boris the Borrower may be guilty of trespass (see trespass above).

Illustrative Example 2: Boris the Borrower "borrows" his neighbor's lawn mower for 5 straight weeks; Boris took the lawn mower from his neighbor's shed without permission. Boris returns the lawn mower in the same condition he found it, with a full tank of fuel. However, while it was missing, rightful owner went to use the lawnmower, noticed it was missing, and purchased a replacement. Boris the Borrower is most likely liable for conversion (and possible trespass; see above) and would be responsible for paying damages.

Damages for Conversion

The law generally allows the injured party to either recover the chattel, seek damages, or both.

When it comes to paying monetary damages for conversion, what standards should the courts apply? Should the tortfeasor pay the original cost the owner paid for the chattel? The present value of the chattel at the time converted? The cost of replacing the chattel? What if the tortfeasor sold the chattel at a significant profit? Being that items may appreciate or depreciate in value over time, these questions are not simple.

The Restatement of Torts (Second) provides general guidance for how much a tortfeasor should pay in damages:

> In determining the seriousness of the interference and the justice of requiring the actor to pay the full value, the following factors are important: (a) the extent and duration of the actor's exercise of dominion or control; (b) the actor's intent to assert a right in fact inconsistent with the other's right of control; (c) the actor's good faith; (d) the extent and duration of the resulting interference with the other's right of control; (e) the harm done to the chattel; and (f) the inconvenience and expense caused to the other. (*Restatement of the Law (Second), Torts §222A*)

In other words, the court will examine the motives and actions of the tortfeasor, taking into account how long and to what extent the tortfeasor's actions deprived the plaintiff to access and rightful enjoyment of his or her chattel. The court will also examine the actual damages or inconvenience to the plaintiff.

Conclusion

Modern tort law has been shaped by almost four thousand years of political, economic, and social trends. The United States has a complex system of civil-based tort law that protects property interests and provides prescribed remedies when damage or injury to property occurs. It is difficult to predict the future of tort law. While tort reform was a significant topic in the latter half of the twentieth century, much talk of major reform has been replaced by tinkering at both the national and state level to make the system more efficient and user friendly for litigants.

Cross-References

► Tort: Property

References

75 Am Jur 2d Trespass §1–§197.
Case of the Thorns (1466) YB 6 Ed 4, 7a pl 18.
Geler v. National Westminster Bank, 770 F. Supp. 210 (1991).
Gould v. Ochsner, 354 P.3d 965 (2015).
Herrin v. Sutherland, 74 Mont. 587, 241 P. 328 (1925).
Iglesias v. United States, 848 F.2d 362 (1988).
Keegan v. Lemieux Security Services, Inc., 177 Vt. 575, 861 A.2d 1135, (Vt. 2004).
Lebovitz v. Sheraton Oper., 868 So. 2d 164 (La. Ct. App. 2004).
Macomber v. Travelers Prop. & Cas. Corp., 261 Conn. 620 (2002)
McTiernan v. Jellis, 316 P.3d 1153 (2013).
Morgan v. High Penn Oil Co, 238 N.C. 185 (1953).
Palm Beach Golf Center-Boca, Inc. v. John G. Sarris, D.D. S., P.A., 771 F.3d 1274 (2014).
Pestey v. Cushman, 788 A.2d 496 (2002).
Peters Griffin Woodward, Inc. v. WCSC, Inc., 88 A.D.2d 883 (1982).
Philadelphia Elec. Co. v. Hercules, Inc., 762 F.2d 303 (1985).
Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766 (2010).
Restatement of the Law (Second), Torts §157–§280.
State v. Girardier, 484 S.W.3d 356 (2015).
State v. Zembreski, 445 N.J. Super. 412 (2016).
Taylor v. Cincinnati 143 Ohio St. 426 (1944).
Taylor v. Forte Hotels Int'l, 235 Cal. App. 3d 1119 (1991).
Thorton v. Schiavello, 93 A.3d 656 (2014).

Further Reading

American Law Institute: Restatement of the Law (Second), Torts §157–§280.
An introduction to American Law: Tort Law (Part 1) University of Pennsylvania. Online Coursera https://www.coursera.org/lecture/american-law/tort-law-part-1-d3d6Q
Schwartz, V. E., Kelly, K., & Partlett, D. F. (2015). *Prosser, Wade, and Schwartzs torts: Cases and materials*. St. Paul: Foundation Press.

W

Workplace: Hostile Environment

Emily Schindeler
Griffith Criminology Institute, Griffith University, Brisbane, QLD, Australia

Keywords
Workplace hostilities · Harassment · Prevalence · Risk · Prevention

Definition

Hostility within the workplace is an umbrella term encompassing behaviors – including harassment, aggression, bullying, emotional and verbal abuse, anti-social behavior, incivility, or abusive supervision – that cause harm to a target as well as to bystanders. In the United States workplace hostility refers specifically to prohibited discriminatory behaviors as administered by the federal Equal Employment Opportunity Commission (EEOC) and set out in civil rights legislation. This is paralleled in the *United Kingdom Equality Act 2010*. Injurious behaviors and targets not falling within the ambit of the legal protections in the anti-discrimination legislation are included in other national jurisdictions such as the *Workplace Health and Safety Act 2011* in Australia.

Introduction

The classification of abusive behaviors within the work environment has been debated by academic researchers, organizational behaviorists, regulators, national and state governments, the European Union, the International Labor Organization, and the World Health Organization. A useful illustration is found in Neall and Tuckey's (2014) review of 234 peer reviewed articles which found 36% adopted workplace bullying, 21.3% workplace aggression, 10% workplace harassment, and 9.2% workplace incivility and abusive supervision each. Irrespective of differences in characterizations, there are commonalities in that behaviors involve intent to do harm, identification of a specific target or targets, and the presence of severe and recurring acts. Protections are grounded in definitions of harm rather than simple offense (PLC Labor & Employment 2014). It is important to recognize that persistent incivility and environmental toxicity (rendering the individual socially isolated and devalued) can lead to the same harm that is ascribed to more aggressive forms of harassment.

However, the nature of terminology has critical repercussions for who may be protected, who is responsible, and under what conditions. Definitions embedded in statutory protections and regulations proscribe specific behaviors and actions, potential reparations for victims, as well as responsibilities of employers.

© Springer Nature Switzerland AG 2021
L. R. Shapiro, M.-H. Maras (eds.), *Encyclopedia of Security and Emergency Management*,
https://doi.org/10.1007/978-3-319-70488-3

For example, by limiting the definition of harassment to a protected characteristic the focus is directed to the individual trait as the basis for the abusive action itself. This demonstrates how the process of definition and consequent parameter setting can result in discrimination against particular victims or protect particular offenders. There is a specific consequence of the specifications adopted in legislation and the locus of responsibility for enforcement. It is in this context that the EEOC Taskforce (2016) did not limit their investigation into harassment to a legal definition recognizing that conduct which is not specifically illegal can create an environment in which unlawful hostilities can occur. Outside of the United States, protections against abusive behavior which causes psychological harm are found in labor laws as well as workplace health and safety laws and regulations (e.g., France, Australia, and Canada).

Conduct characteristic of hostility in the workplace sits apart from physical assault which is illegal under criminal law. In the United States, conduct subject to EEOC protections involve discrimination against the individual(s) target based upon age, race, religion, sex, national origin, or disability. Legal requirements demand that discrimination must be ongoing over time; involve behavior that a reasonable person would find intimidating, hostile, and abusive; and evidence that such treatment interferes with the individual's ability to work and career advancement. Further, the target is required to report to the employer of the complaint. The employer then becomes liable for any failure for inadequately intervening. Retaliatory discrimination against a person who has filed a charge of discrimination or been involved in investigation or testifying in such cases is also unlawful. The U. S. Occupational Safety and Health Administration has an interest in the protection of workers but limited regulatory or enforcement powers specific to workplace hostilities as compared with physical violence (https://www.osha.gov/SLTC/workplaceviolence/standards.html). Accordingly, while federal protections are provided for a target having a specified attribute, a victim who is not captured by the civil rights provisions has significantly diminished protection.

Abuse consistent with definitions of hostility in the work environment may be perpetrated by those in positions of authority, peers, or subordinates. Individuals or groups of individuals may be involved as perpetrators and victims may include not only the target but also bystanders. As noted by Reynald (2016), bystanders are inclusive of those who witness victimization and those who are in receipt of official reporting within the organization and regulators responsible for action. Bystanders may become secondary victims as well as having a potential capacity to act as an intervener. Those factors that may inhibit victim's reporting are equally applicable to the bystander. These include a fear of becoming a target, lack of confidence that management would be supportive or take action, unsure whether co-workers would support the action and concern for the lack of personal protection against risks (Wortley 2015). Perceived seriousness of the behavior, closeness to the target, and perceived personal responsibility to act will also influence bystander responses. An organizational culture which accepts if not condones such mistreatment is also a powerful inhibitor to action being taken (Pershing 2003; D'Cruz and Noronha 2010). While legislated protections focus on those employed by an organization, abuse may also emanate from third parties such as clients, patients, and consumers and which is not covered by legislated protections.

Prevalence

Determining the prevalence of workplace hostilities is fraught by confounding factors. Under-reporting may be a consequence of a victim's fear of taking action given the employment risks, victims may elect to leave the workplace to escape the situation, and victims may simply be unaware of their rights (Schindeler 2016). National, industry specific and specialist prevalence studies have adopted selected definitions, collection, and measurement tools. Methodologies have ranged from those based on unfettered self-reporting of experiences perceived as hostile, reporting according to

specific (but often different) criteria, applying measurement tools based on behavioral characteristics, and/or consequences. For this reason, it is not possible to produce comparative studies given the lack of consistency in definitions, criteria, and methodology. Acknowledging these limitations, recording a small number of prevalence studies is useful in demonstrating the relevance of the problem.

Recognizing the need for greater attention to workplace mistreatment, the National Institute for Occupational Safety (NIOSH) and Health and the Centres for Disease Control and Prevention (CDC) initiated the inclusion of relevant questions in the 2010 *National Survey of Workplace Mistreatment and Absenteeism* (Asfaw et al. 2014). Some 13,000 respondents to the National Health Interview Survey were asked, "During the past 12 months, were you threatened, bullied, or harassed by anyone while you were on the job?" The responses to this question revealed that 7.6% of US workers employed at the time of the survey (2010) had been mistreated at their workplace. Some five years later, the EEOC *Select Task Force on the Study of Harassment in the Workplace* (Feldblum and Lipnic 2016) reported that an allegation of harassment accounted for nearly one third of the 90,000 employment discrimination charges received by the EEOC in 2015. These two studies approached understanding prevalence from different perspectives and therefore cannot be directly equated. For example, the Task Force was able to look at formal complaints of discrimination as well as drawing on complementary studies as compared to the single NIOSH and CDC survey. Examining incidence based upon the employment sectors, the Task Force found that allegations of harassment centered on sex and race were most prevalent in the private sector, accounting for 45% and 34% of charges, respectively. In contrast, allegations of harassment based on race and disability were most prominent in the public sector, accounting for 36% and 34% charges, respectively.

A corollary to being a direct target of hostility is the need to recognize the flow on impact on bystanders. In the Danish national cohort study set out in *Working Environment and Health in Denmark 2012–2020* (Nielsen and Moller 2012) and the *Finnish Quality of Work Life Survey* (OSF 2008) that the proportion of respondents witnessing hostile behaviors increased greater than the number reporting victims of such abuse. These studies reported that bystanders experienced similar levels of psychological harm as a consequence of witnessing the mistreatment to others. This can result in health impacts of increased stress, in the need to change workplaces completely, as well as emotional distress. There are consequential flow on costs to the organization and productivity.

Environmental Risk Factors

Two theoretical positions are linked to risk factors as the principle causes of hostilities within the workplace and the types of preventative and intervention strategies that are often promoted. The first locates the source of hostilities as grounded in inter-personal conflict which can be addressed through strategies designed to prevent or respond to such clashes. The abusive supervisor or workplace psychopaths are expressions of this thinking. The alternative explanation views workplace is a result of cultural and systemic factors inherent in the organisation. Recognizing that environmental conditions can be conducive to individual behaviors; these two explanatory frameworks are not mutually exclusive (Eurofound 2015). The relationship between organizational culture and individual factors is brought together by Sallin (2003). In this model, enabling and motivating structures or inducements and specific events interact creating the ideal conditions for workplace hostilities. This also indicates that prevention and intervention techniques need to be tailored to organizational environments, at different levels and with different characteristics.

Internal organizational factors which may increase the potential for hostility in the workplace involve a combination of influences within the ability to be mediated by the employing organization. Any or all of these organizational characteristics may intensify the level of risk of

unacceptable and harmful inter-personal behaviors. Management styles will set the overall organizational culture. Autocratic leadership styles, lack of accountability for decision–making, and promotion of a divisive work culture are all risk factors (Hoel et al. 2010; Ferris et al. 2007). Poor leadership may generate risk in the form of system failures. System failures may include providing inadequate resources, making unreasonable performance demands, failing to provide adequate support, and poor communication. Broadly categorized as work-related factors linked to risk include tolerance of unreasonable behavior, job insecurity, role conflict, and ambiguity, as well as organizational change.

The manner by which managerial practices are implemented such as performance assessment, performance management, the provision of incentives, and a lack of disincentives will impact on the perception of fairness. When processes are viewed as unreliable or unfair, they become a risk factor for harm. Performance appraisal and management have been promoted as a constructive way of addressing problems in productivity or quality of work. At the same time, these processes have been associated with claims of abuse – that is the process has been used as tactic for victimizing individuals and harm-inducing. As a reflection of the organizational climate, the application of management practices may be effectively abusive or supportive. Organizational practices which reinforce abusive behaviors by providing justifications enable such practices to persist (Piquero 2005).

Failure of the organization to provide credible responses to complaints is a significant risk factor. Supervisors or managers and human resource staff failure to deal with complaints, which adopt an approach that blames the victim or that is tacitly supportive of the accused can lead to an actual increase in workplace hostilities. Where implementation of policies and procedures is perceived as ineffective and those responsible for taking action are not trusted, there is reduced likelihood that victims or bystanders will report the offending behavior (Reynald 2016; Wortley 2015). Observing how an organization responds to victims of workplace hostilities may communicate that such abuse is "part of the job," intensify the stressors and increase the nature of risk (Hoobler and Swanberg 2006).

The climate which emerges from the interaction of organizational power and politics produces environments conducive to workplace hostilities, culminating in a form of systemic abuse. This can have the profound impact on normalizing what is harmful even if not illegal behavior (Leiter and Patterson 2014).

Prevention and Intervention

There is no single recipe which will ensure protection against workplace hostilities. There are pre-requisites without which prevention is unlikely to be successful. For example, policies and procedures that address specific behaviors in isolation are inadequate. There is a need for an organizational culture, ethical framework, and accountable, reliable systems to reduce the risk of workplace hostilities. Similarly the EEOC Special Task Force (Feldblum and Lipnic 2016) identified a number of workplace characteristics that are linked to risk and for which particular responses are suggested. For example, homogeneity and diversity of workplaces and the evidence of specific vulnerable groups are identified among risk factors. Effective prevention requires leadership to convey the values and ethics of the organization, in both the private and public sectors.

The processes associated with risk assessment and development of prevention and intervention strategies need to be inclusive. This requires the involvement of both management and those working at the ground level. Effective prevention demands ongoing monitoring to identify emerging risks and a willingness to take remedial action. For example, the emergence of social media as a site for targeted abuse represents an emerging risk for which online training programs are accessible, primarily through the private sector providers. However, there has not been any robust evaluation of their effectiveness. Evaluation of the effectiveness of prevention and intervention actions similarly needs to be inclusive, form part

of the monitoring process and strategies focused on cultural change. An over-reliance on complaints is an insufficient measure of the effectiveness of strategies given the imposts to victim or bystander complaints.

The features of any intervention must be tailored to respond at least one or more risks. Primary interventions are preventative and are primarily organization-focused. Awareness raising activities, leadership development, and identifying systemic factors contributing to risk fall within this category of intervention (Vartia and Leka 2011). For example, leadership development approaches focusing on enhancing the quality or culture of the work environment are potentially influential in reducing risk even when workplace hostilities may not be the ostensible goal. Risk may also be reduced when action is taken to reduce work-related stress through work design, organizational practices, and improve communication even where not positioned from the perspective of reducing hostilities (Ng et al. 2014).

Secondary interventions are intended to improve responses to identified risks. This includes such actions as promoting behavioral change and individual resilience as related to group dynamics. Improving internal processes, including the operation of human resource management practices, are included in this level. Interventions involving the adoption of risk assessment tools and providing coal face training including involving interpersonal skill development have promoted as options. However, there is a paucity of evaluations that have demonstrated sustainable outcomes for such initiatives (Hoel and Giga 2006; Hodgins et al. (2014); Evesson and Oxenbridge 2015).

Tertiary interventions must provide effective outcomes for victims as well as appropriate responses to perpetrators. Both organizational wide and targeted approaches must address context relevant risk factors. Repairing the harm after the fact requires attention to recovery for individuals and work groups. This includes providing remediation for the victims (including bystanders impacted while not the direct target) as well as addressing the risks which enabled the offending to occur. Critically, the events which led to the abuse and identification of the factors that enabled it to occur are then able to be employed in reviewing the organization's prevention strategies (US Merit Systems Protection Board 2012; Safe Work Australia 2013).

An alternative framework is to categorize the nature of actions being taken as organizational, administrative, or behavioral. Organizational and administrative actions may include, for example, adoption of relevant policies and procedures, developing programs, or addressing ways to improve work management systems. Behavioral focused actions may include for example awareness raising campaigns, interpersonal skill development (e.g., managing aggression or conflict management), or communication skills.

Codes of practice, guidelines, and advisory notes provide common processes or approaches to assist organizations to development strategies for prevention and intervention (Safe Work Australia 2013; Department for Business Innovation and Skills 2009; US Merit System Protection Board 2012). Elements which are commonly included are engagement, risk assessment, controlling of risks, and responding to incidents. Engagement provides the means by which critical environmental factors are able to be identified and advise locally appropriate responses. Risk-assessment tools direct consideration to potential work-related stressors, systemic problems, and management styles. Monitoring patterns of absenteeism, sick leave, and complaints provide additional data indicating risk. Controlling of risks then can be directed towards those elements which have been identified as problematic. Finally processes for responding to incidents and complaints which provide remedial action and recovery are the critical components of the overall prevention strategy.

Conclusion

There are significant gaps in research that require attention. The problem of investigating claims, the problem of evidence, and the responsibility of victims to produce "credible evidence"

remain problematic as does the transparency of decision-making. Greater clarity as to what constitutes evidence and how it will be collected and assessed is needed for victims, bystanders, investigators, and managers. An accountable investigatory and decision-making process which establishes greater clarity of responsibility is needed. This gap includes limited evidence of the effectiveness of approaches that focus not on the victim but on the perpetrators. There is a paucity of robust evidence of the long-term effectiveness of any of the interventions that are widely promoted, particularly in organizations that have prior experience with workplace hostility problems. This will necessitate a continuing focus and collaborative approach with employers and regulators to test and document the quality and sustainability of actions.

Cross-References

- ▶ Workplace Violence: Assault
- ▶ Workplace Violence: Factors Contributing and/or Facilitating
- ▶ Workplace Violence: Sex-Related Crimes

References

Asfaw, A., Chang, C., & Ray, T. (2014). Workplace mistreatment and sickness absenteeism from work: Results from the 2010 National Health Interview Survey. *American Journal of Industrial Medicine, 57*(2), 202–213.

D'Cruz, P., & Noronha, E. (2010). The exit coping response to workplace bullying. *Employee Relations, 32*(2), 102–130.

Department for Business Innovation and Skills. (2009). *Preventing workplace harassment and violence: A joint guidance implementing a European social partner agreement*. Britain: BIS.

Eurofound. (2015). *Sixth European working conditions survey*. Luxembourg: Publication of the Office of the European Union Feldblum.

Evesson, J., & Oxenbridge, S. (2015). *Seeking better solutions tackling bullying and ill treatment in British workplaces*. UK: ACAS. Retrieved from online http://www.acas.org.uk.

Feldblum, C. R., & Lipnic, V. A. (2016). *Report of the co-chairs of the EEOC select task force on the study of harassment in the workplace*. Washington, DC: U.S. Equal Employment Opportunity Commission.

Ferris, G., Zinko, R., Brouer, R., et al. (2007). Strategic bullying as a supplementary, balanced perspective on destructive leadership. *The Leadership Quarterly, 18*(3), 195–206.

Hodgins, M., MacCurtain, S., & McNamara, P. (2014). Workplace bullying and incivility: A systematic review of interventions. *International Journal Workplace Health Management, 7*(1), 54–72.

Hoel, H., & Giga, S. (2006). *Destructive interpersonal conflict in the workplace: The effectiveness of management interventions*. UK: British Occupational Health Research Foundation (BOHRF).

Hoel, H., Glas, L., Hetland, J., Cooper, C., & Einarsen, S. (2010). Leadership styles as predictors of self-reported and observed workplace bullying. *British Journal of Management, 21*(2), 453–468.

Hoobler, J., & Swanberg, J. (2006). The enemy is not us: Unexpected workplace violence trends. *Public Personnel Management, 35*(3), 229–246.

Leiter, M., & Patterson, A. (2014). Respectful workplaces. In A. Day, J. Hurrel, & E. Kelloway (Eds.), *Workplace well-being: How to build positive psychologically healthy workplaces* (pp. 205–261). Chichester: Wiley.

Maestas, N., Mullen, K. J., Powell, D., von Wachter, T., & Wenger, J. B. (2017). *Working Conditions in the United States: Results of the 2015 American Working Conditions Survey*. Santa Monica: RAND Corporation.

Neall, A., & Tuckey, M. (2014). A methodological review of research on the antecedents and consequences of workplace harassment. *Journal of Occupational and Organizational Psychology, 87*(2), 225–257.

Ng, J. L., Johnson, A., Nguyen, H., & Grot, M. (2014). *Workplace culture improvements: A review of the literature*. A report for the workforce planning development branch of the NSW.

Nielsen, M., & Moller, S. (2012). *Working environment and health in Denmark 2012–2020*. Copenhagen: National Research Centre for the Working Environment.

Official Statistics of Finland (OSF). (2008). *Quality of work life survey [E-Publication]*. Helsinki: Statistics Finland Access method. https://www.stat.fi/meta/til/tyoolot_en.html.

Pershing, J. (2003). "To snitch or not to snitch?" applying the concept of neutralisation techniques to the enforcement of occupational misconduct. *Sociological Perspectives, 46*(2), 149–178.

Piquero, N. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behaviour: An Interdiscplinary Journal, 26*(2), 159–188.

PLC Labor & Employment. (2014). Workplace Violence, Practical Law Practice Note 7-505-7511 (2014). WestLaw: Next, Thomas Reuters.

Reynald, D. (2016 [2017]). The conundrum of bystanders to psychological abuse in the workplace: From passive accomplices to active controllers. In E. Schindeler, J. Ransley, & D. Reynald (Eds.), *Psychological violence in the workplace: New perspectives and shifting frameworks*. London: Routledge.

Safe Work Australia. (2013). Guide for preventing and responding to workplace bulling. Online http://safeworkaustralia.gov.au

Sallin, D. (2003). Ways of explaining workplace bullying: A review of enabling, motivating and precipitating structures and processes in the work environment. *Human Relations, 56*(10), 1213–1232.

Schindeler. (2016 [2017]). Prevalence – What to count, how and the influence of the narrative. In E. Schindeler, J. Ransley, & D. Reynald (Eds.), *Psychological violence in the workplace: New perspectives and shifting frameworks*. London: Routledge.

U.S. Merit System Protection Board. (2012). Employee perceptions of e Workplace Violence, A Report to the President of the United States. Washington, DC.

Vartia, M., & Leka, S. (2011). Interventions for the prevention and management of bullying at work. In S. Einarsen, H. Hoel, D. Zapf, & C. L. Cooper (Eds.), *Bullying and harassment in the workplace* (pp. 359–380). New York: CRC Press.

Wortley, R. (2015). Whistle-blowers as capable guardians: The decision to report wrongdoing as a (bounded) rational choice. In M. A. Andresen & G. Farrell (Eds.), *The criminal act: The role and influence of routine activity theory* (pp. 196–213). Basingstoke/Hampshire: Palgrave Macmillan.

Further Reading

Einarsen, S., Hoel, H., Zapf, D., & Cooper, C. L. (Eds.). (2011). *Bullying and harassment in the workplace*. New York: CRC Press.

Equal Employment Opportunity Commission. (2016). *Report of the Co-Chairs of the EEO select task force on the study of harassment in the workplace*. US: EEOC.

Jenkins, M. (2013). *Preventing and managing workplace bullying and harassment: A risk management approach*. Toowong: Australian Academic Press.

Schindeler, E., Ransley, J., & Reynald, D. (2016). *Psychological violence in the workplace: New perspectives and shifting frameworks*. London: Routledge.

Workplace: Privacy

Kenneth J. Grossberger
John Jay College of Criminal Justice, New York, NY, USA

Keywords

Privacy · Workplace · Expectation of privacy · Search · Probable cause · Reasonable · Employee monitoring · Surveillance · Risk

Definition

Privacy in the workplace refers to an employee's presumptive right to limited privacy including use of the organization's phones, computers, desks, lockers, and other equipment, in accordance with that organization's legal rules and policies.

Introduction

This article discusses privacy in the workplace and the privacy protections of the 4th Amendment to the US Constitution.

Privacy is an assumed right that is not implicitly mentioned in the US Constitution. It can be inferred from several sections of the constitution, most notably the 4th Amendment. A number of US Supreme Court cases support this. The 4th Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (Cornell Legal Information Institute (2) n.d.)

Privacy Rights and Limitations in the Workplace

Limitations

Privacy rights are protected by federal and state laws, as well as regulations. These rights exist in the workplace but are limited. Cooper (2012) expresses this idea by stating that "Americans have as citizens enjoyed certain rights that they are required to leave behind when they enter the doors of the organizations in which they work." These rights are, most notably, "freedom of speech, press, and assembly; due process of law; privacy; and freedom of conscience," and, to the point, "most Americans are not guaranteed these rights in the workplace" (Cooper 2012)

Expectation of Privacy

Employees generally enjoy a reasonable expectation of privacy on the workplace, but the word

"reasonable" requires some definition (Justia n.d.). Legally, the concept is based on what would be reasonable under certain circumstances that would otherwise be considered unusual or require a warrant issued by a court for intervention (Justia n.d.).

The general principal is that searches of an employee's workspace, or of equipment and technology used by the employee, are justified only under certain circumstances. Managers and supervisors have limited rights to search employee occupied areas or organizational equipment employees use. These would include physical spaces such as desks and lockers, and technology such as computers, email, and phones. Any searches of areas used personally by employees must be for valid reasons, either for probable cause (a high evidentiary standard) or reasons that fall under the organization's policies. This usually requires prior notice to the employees unless there is substantive evidence of fraud or wrongdoing by that employee, or the employee has given consent. Reasonableness also does not usually require a warrant for searches whose purpose is to obtain job-relevant material (Berman et al. 2016).

The expectation of privacy is a pervasive issue as employees generally seek a level of comfort in the workplace and do not wish to have their job spaces intruded upon. Exceptions to this would be secure areas in government and research where closer scrutiny is part of the culture. In general, however, the human resources department must ensure that the "need for the monitoring is supported by a legitimate business justification and that employees understand they have no reasonable expectation of privacy when they are using employer-provided equipment and systems" (Society for Human Resource Management n.d.). Thus, the human resources strategy is to provide a personnel comfort level with searches by ensuring that reasonable notice of searches is given.

Legal Issues

Overview

The 4th amendment protects against illegal search and seizure. In the workplace this is problematic as there is a conflict between employer rights to control the organization's property and the limited privacy rights of the employee. The right to privacy in the workplace continues to be controversial as employers can control an employee's workspace and the employee's means of communication (Berman et al. 2016, p. 119). The additional complicating factor here is the employer's technology, which is used by the employee but controlled by the employer.

The employer's property rights further conflict with the employees' privacy rights when organizational communications are checked, thus while monitoring an employee's communication may impinge on his or her privacy the employer may engage in such activity as long as the employee are given notice (Berman et al. 2016, p. 119). This practice may also include private conversations in employer owned spaces. Workspaces such as desks and lockers may be considered more controversial as the expectation of privacy may be greater in those areas despite court cases favoring the employer (O'Connor v. Ortega 1987). Testing for drug use is also a point of concern unless prior consent is obtained or probable cause of crime exists (Society for Human Resource Management n.d.).

Disgruntled employees who feel their rights have been violated can bring actions against employers. Lawsuits and claims can be costly and time consuming. Employers might spend valuable resources and managerial time defending against such actions. Employee relations can worsen and the employers may also suffer reputational damage from negative publicity. Adverse information obtained by employee monitoring can also lead to discipline, termination, or loss of money and benefits. These consequences are burdensome, cost time and money, and must be calculated when forming policies and engaging in monitoring activities.

Relevant Cases

There are numerous cases involving employees' privacy rights and limitations in the workplace. In the US Supreme Court case O'Connor v. Ortega (1987), the issue of searches in an employee's desk was decided. "Conflicts arise when people feel that managers invade their private affairs or private workspaces," as problems occur when the

search is unreasonable (Berman et al. 2016), p. 2018. Employers are restricted from such "unreasonable" searches where the employee has a "reasonable expectation of privacy" in such areas as desks, lockers, and file cabinets (Berman et al. 2016, p. 118).

But employees do not have the same privacy rights when using company email systems, even if such communications are usually considered privileged, as decided in US v. Hamilton (EPIC.org n.d.). In this case, the Court decided that the employer's (in this case the government's) right to access emails outweighed the employee's privacy interests.

Probable cause (a high standard of evidence) was superseded by the "reasonable suspicion" standard in the 1968 US Supreme Court case of Terry v. Ohio (Cornell Legal Information Institute (3) n.d.). This premise applies to places of business as well as homes and public places (Cornell Legal Information Institute (3) n.d.). Reasonable suspicion is a concept the Supreme Court judged as necessary to enable law enforcement to determine if searches were justifiable under certain conditions. A police officer may act if he or she reasonably suspects someone has committed or is about to commit a crime. The extension of this principle in the workplace is that an employer does not need probable cause to conduct a search of an employees' desk or emails if justifiable policy allows it or exigent circumstances exist. The specific situational factors determine the viability of the employer's search (EPIC.org n.d.).

The reasonable expectation of privacy issue was addressed in Katz v. US (1967) in which the US Supreme Court provided further substantiation of the legal parameters for a search and an employee's right to privacy. The Katz ruling updated and amended the judgments of previous court cases and extended privacy protections "to all areas where a person has a reasonable expectation of privacy" (Tokson 2016). For example, the court determined that "immaterial intrusion" involving technology would now be considered a search (Tokson 2016). This case provides what is known as the two-part Katz Test, which says that "first is that the plaintiff displayed an expectation of privacy" and then that "the second is that this expectation is 'reasonable'" (Tokson 2016). This test may apply to the workplace.

Searches – Consent

Employee consent to a search can be implied or in writing. However, implied consent applies when "surrounding circumstances exist that would lead a reasonable person to believe that this consent had been given, although no direct, express, or explicit words of agreement had been uttered" (Cornell Legal Information Institute (1) n.d.). Written consent must be in a form that would prove valid in a court of law. When an employee consents to a search or to provide personal information, then the right to privacy has been waived.

Organization policies on the use of office space, furniture, communications, and equipment is usually in writing, and often employees must sign a document indicating they understand, and consent to, such policies. In those cases, the employees' rights to privacy is usually considered waived. Further, if the employee signed an agreement upon employment allowing the employer to search employee occupied areas, or the employee's emails or phone records, or take and use photos or images of the employees, then consent in those circumstance is again usually considered waived as well.

However, in the case of government employees, the "employer's control of the premises and the equipment, the implied consent of the worker who is generally informed that monitoring might take place. . .. . .combine to greatly limit a government employee's reasonable expectation of privacy" (Rothstein 2000).

HIPAA

The Health Information Portability and Accountability Act of 1996 (HIPAA) provides that employees' health information must be kept confidential by an employer. "The Privacy Rule, a Federal law, gives you rights over your health information and sets rules and limits on who can look at and receive your health information" and thus provides a layer of protection for employees (US Department of Health and Human Services n.d.). Further "the Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral" and

"the Security Rule is a Federal law that requires security for health information in electronic form" (US Department of Health and Human Services n.d.). Therefore, there are strong regulations that safeguard personnel medical information, and usually human resources departments are responsible for this. This is especially true for medical insurance files and claims by employees. These regulations restrict access by third parties without good cause or a court order (US Department of Health and Human Services n.d.).

Workplace Privacy – Physical

Office Spaces, Desks, and Lockers

These assets are assigned by the employer to specific employees, as differentiated from to public areas and equipment for use by many, or all. As mentioned above, the privacy rights for these employer-owned items are often assumed by employees or equipment is used without consideration of consequences. People in offices typically do not think about their private or personal use of these items. Employer searches of these areas, absent specific consent or notice, can therefore cause resentment, complaints, or claims and lawsuits. This is undoubtedly more of an issue if the employee has been working in that organization for a longer period of time. Privacy rights are usually not a concern until a worker is confronted with a search (Katz v. US 1967).

Drug Testing

Drug testing is often a controversial intrusion into an employee's job. Such testing is sometimes required at hiring as a condition of employment, and often used randomly to see if staff is engaging in illegal use of controlled substances. The general premise is that "an employer may be able to require its employees to submit to drug screening" (Society for Human Resource Management n.d.). Written consent is required, unless there is probable cause, for example, discovery of drugs or drug paraphernalia or knowledge of "workers whom management believe have been using drugs based on physical evidence or behavior" such as glassy eyes or slurred speech. (Society for Human Resource Management n.d.). This testing is typically the responsibility of human resources. There are issues with random testing as some employees may feel targeted, resulting in disparate treatment claims (i.e., being treated differently for illegal reasons) (Nolo.com n.d.). There are also practical issues as to how and when the testing would be done, and the custody and control of the evidence. Most drug tests as of this writing are saliva tests (which are less problematic than urine tests) and can be done on premises.

Workplace Privacy – Technology

An employee's privacy has become more problematic as "the increased use of technology in the workplace has created new concerns for both employers and employees in the area of privacy" (Beekman Center for Internet and Privacy n.d.). Employers own or control the technology used by the employees in the workplace, which includes the Internet, cameras, voicemail, telephones, email, computers (desktops, laptops, tablets), cell phones, office phones, and other electronic communications.

Computers

Employees use equipment such as computers and PDAs (Personal Digital Assistants) that belong to the employer. While they have permission to use such equipment, they do not own it, and their use of it is therefore subject to the rules of the employer. Personal use of this equipment may be allowed but may subject to employer scrutiny. Here is where the grey area exists and the risk of conflict increases.

Documents and data on these devices may be the product of the employee but is generally considered to be owned by the employer, even if such data is of a personal nature. Employer systems are subject to the owner's property rights which typically supersede any privacy rights presumptions (Skok 1999). Thus, the employees' privacy rights may be diminished.

Internet Usage, Clickstream Data, and Email

Emails and data sent through the employer's "electronic information network" is generally considered to be the employer's property (Society for Human Resource Management n.d.). However, "once an expectation of privacy is established in clickstream data" Fourth Amendment protections involving "the reasonableness of searches and seizures" readily attach (Skok 1999).

Workplace users of clickstream data on the Internet are subject to employer intrusion, despite a reasonable expectation of privacy of the employee (Skok 1999). While such intrusions, or searches, must be reasonable and mindful of an individual's Fourth Amendment rights, the employer can argue a compelling interest despite protection of the courts against such "overly extensive and indiscriminate intrusion into our online lives" (Skok 1999). Employer systems can check emails with little impunity as employee suits "have not enjoyed much success" (Society for Human Resource Management n.d.). In addition, employer's use of such data is problematic as such employers must be "mindful of the discoverability of electronic communications" (Society for Human Resource Management n.d.).

Phone Calls and Voice Messages

The same is true for phone calls as employers may monitor such communications if there is a compelling need, the employee is given notice, or probable cause exists (Berman et al. 2016). Employers have access to voice messages collected and stored by the employee as well, but such monitoring is still the subject of controversy.

Employee Monitoring

Employers may have legitimate and compelling reasons for collecting information about their employees such as "guarding trade secrets," "monitoring for performance indicators," and bad behavior, risk management issues and evidence of prior illegal acts (Beekman Center for Internet and Privacy n.d.). The interest of the organization is served when "data about employee performance, for instance, can be used for better planning and resource allocation" or where more employee training is necessary.

(Beekman Center for Internet and Privacy n.d.). However, this "information could unnecessarily damage an employee's reputation with an employer or cause unneeded suspicion" and distrust, and this is one of several issues where the legitimate violation of an employee's privacy can cause more harm than good (Beekman Center for Internet and Privacy n.d.). Data obtained by employee surveillance is another problem-laden issue, and even if for internal use, this method of information collection may carry significant risk (Beekman Center for Internet and Privacy n.d.).

The liability created by employee monitoring is potentially costly as "conflicts arise when people feel that managers invade their private affairs or private workspaces". Trust is an important element in employee relations and may be compromised as employee monitoring changes the equation between the organization and its workers by "questioning employee rights to privacy, autonomy, and respect". Organizations may use electronic monitoring technology such as surveillance cameras usually without notice to employees if used in public places (bathrooms are not allowed), as there is no reasonable expectation of privacy in such spaces. However, the practical issues of employee resentment, lawsuits and claims, and turnover, put stress on human resources departments. Employers therefore need a reasoned approach to search and monitoring policies.

Employers may use technology to manage their exposures "to prevent injuries, misconduct and other types of loss" (Society for Human Resource Management n.d.). Organizations may also be concerned by business risks and threats, despite privacy concerns, and may then decide "to track all employee e-mail, Internet and telephone use without employees even knowing that they are being monitored" (Society for Human Resource Management n.d.). In many of these cases, employers must heed laws requiring notice

of monitoring as privacy rights may be affected, and legally advising employees of such surveillance is the most prudent course (Society for Human Resource Management n.d.).

Further, employers may monitor phone calls and access voice mail as part of normal course of business but not without good reason (Society for Human Resource Management n.d.). Employers also have the right to track and manage employees' use of the organization's Internet (Berman et al. 2016). Many of these interactions fall under the Electronics Communications Privacy Act (ECPA) which limits the employers ability to intrude in workers phone conversations. For example, an organization usually cannot engage in surveillance of employee's telephone usage, even if on the organization's equipment (Society for Human Resource Management n.d.). To complicate matters, the ECPA protects the employee's privacy in the use of such technology as, generally, the employer is at risk as the law "generally prohibits unauthorized and intentional 'interception' of wire, oral, and electronic communications. . ." (Beekman Center for Internet and Privacy n.d.). The ECPA additionally guards employee rights as it basically precludes "unauthorized 'accessing' of electronically stored wire or electronic communications" (Cornell Legal Information Institute (1) n.d.). However, the ECPA includes a number of exceptions to these rules including the "*business purpose exception*, which permits employers to monitor oral and electronic communications as long as the company can show a legitimate business purpose for doing so" (Society for Human Resource Management n.d.). Another is the *"consent exception" wherein an employee provides the employer with consent for such monitoring* (Society for Human Resource Management n.d.).

Analysis and Conclusion

Privacy as a practical matter is based more on transactional elements than philosophical legal notions. However, the risk and liability of searches and employee monitoring are significant and must be mitigated by well-considered policy and sound legal advice. "Overall, the majority of employers monitor the activities of their subordinates in some form, and clandestine observation is widespread". However, given the advances in technology, the temptation for employers is to increase surveillance and information collection thus mitigating the employees' rights to privacy while increasing the risks for the employer. This presents challenges for employers and employees alike, and the struggle for balancing the needs of both will continue into the future until the courts can shed more light on this very grey area.

References

Beekman Center for Internet and Privacy. (n.d.). Privacy in cyberspace. http://cyber.harvard.edu/privacy/Module3_Introne w.html

Berman, E. M., Bowman, J. S., West, J. P., & Van Wart, M. R. (2016). *Human resource management in public service: Paradoxes, processes, and problems*. Sage, Los Angeles, CA.

Cooper, T. L. (2012). *The responsible administrator: An approach to ethics for the administrative role*. Jossey-Bass, San Francisco, CA.

Cornell Legal Information Institute (1). (n.d.). Implied consent. https://www.law.cornell.edu/wex/implied_consent

Cornell Legal Information Institute (2). (n.d.). Fourth Amendment. https://www.law.cornell.edu/constitution/billofrights#amendmentiv

Cornell Legal Information Institute (3). (n.d.). Terry v. Ohio. https://www.law.cornell.edu/supremecourt/text/392/1

EPIC.org. (n.d.). Workplace privacy. https://epic.org/privacy/workplace/

Justia. (n.d.). Search and seizure. https://www.justia.com/criminal/docs/search-seizure-faq/

Katz v. United States, 389 U.S. 347 (1967).

Nolo.com. (n.d.). Disparate treatment discrimination. https://www.nolo.com/legal-encyclopedia/disparate-treatment-discrimination.html

O'Connor v. Ortega, 480 U.S. 709, 716 (U.S. 1987).

Rothstein, L. (2000). Privacy or dignity? Electronic monitoring in the workplace. *New York Law School Journal of International and Comparative Law Rothstein, 19*, 379.

Skok, G. (1999). Establishing a legitimate expectation of privacy in clickstream data. *Michigan Telecommunications and Technology Law Review, 6*, 61.

Society for Human Resource Management. (n.d.). Workplace privacy. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx

Tokson, M. (2016). Knowledge and Fourth Amendment Privacy. Scholarly Commons Law, Northwestern University. 111(1).
U.S. Department of Health & Human Services. (n.d.). Your rights under HIPAA. https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

Workplace: Sexual Harassment

Duygu Biricik Gulseren and E. Kevin Kelloway
Department of Psychology, Saint Mary's University, Halifax, NS, Canada

Keywords
Workplace sexual harassment · Gender harassment · Sexual coercion · Workplace aggression

Definition

Workplace sexual harassment is a type of workplace aggression that is defined as "conduct as unwanted or unwelcome, and which has purpose or effect of being intimidating, hostile, degrading, humiliating or offensive" (McDonald 2012, p. 14).

Introduction

The phenomenon of workplace sexual harassment was first identified as an occupational problem in the 1970s, and it has received a great deal of attention from researchers, practitioners, and the media ever since. Although there has been a decrease in the number of formal complaints of workplace sexual harassment in the last decade (Quick and McFadyen 2017), it continues to be a significant problem for both organizations and individuals. Victims of workplace sexual harassment suffer from a wide range of mental health problems that are difficult to treat. Similarly, organizations face a significant amount of productivity loss on top of costs associated with litigation and human rights complaints.

There are at least three approaches to defining workplace sexual harassment: (1) legal, (2) sociopsychological, and (3) public (Cortina and Berdahl 2008). The legal definition of workplace sexual harassment may differ depending on the legislative jurisdiction. For example, the Equal Employment Opportunity Commission's definition recognizes unwanted sexual conduct as workplace sexual harassment if it results in negative work outcomes, such as decreased performance (Quick and McFadyen 2017). The sociopsychological definition of workplace sexual harassment relies on targets' perception of behaviors regardless of the outcomes. Finally, the public definition of workplace sexual harassment is less precise and typically focuses on conduct that is generally accepted as sexually offensive by the public. Workplace sexual harassment behaviors can be categorized in three major groups: (1) gender harassment (e.g., misogynistic comments), (2) unwanted sexual attention (e.g., unwanted physical contact or sexual comments), and (3) sexual coercion or quid pro quo (e.g., asking for sexual favors in exchange for an organizational resource or decision) (Fitzgerald et al. 1997).

About 50% of women and 30% of men were estimated to be victims of workplace sexual harassment in the American workforce (McLaughlin et al. 2012). The comparable figures are much smaller in Scandinavian countries (i.e., a total of 2% of working women in Sweden and 11% of working women in Denmark have been victims of workplace sexual harassment) (Timmerman and Bajema 1999); but much higher in Austria (i.e., workplace sexual harassment victims make up 80% of all women workers in the workforce) (Timmerman and Bajema 1999) than the American statistics. Sexual harassment is a more common problem in gender-imbalanced industries, such as military or healthcare. For example, Estrada and Berggren (2009) found that 84% of the female cadets from a sample of Swedish military personnel experienced at least one episode of workplace sexual harassment within the last 2 years of the study. Working for the military is a risk factor of sexual harassment for men as well. Evidence shows that men are ten times more likely to be exposed to workplace

sexual harassment in a military setting than in other industries (Quick and McFadyen 2017).

The majority of workplace sexual harassment incidents are perpetrated against female employees by their male managers or co-workers (Quick and McFadyen 2017). Although women are generally exposed to more harassment than men, men and members of the LGBTQ community also experience workplace sexual harassment (McDonald 2012). At least some of this gender difference in workplace sexual harassment may be attributable to stigma that discourage men to report it (Kime 2014). The United States Equal Employment Opportunity Commission's (2012) data showed that the number of workplace sexual harassment complaints by men had increased 15.3% between 1997 and 2011. Quick and McFadyen (2017) surmised this rise may be due to reduced stigma around the topic of men's sexual harassment in recent years. Workplace sexual harassment due to one's sexual orientation is even more prevalent than harassment of women and men per se because there is no legal protection for LGBTQ workers in many countries, and the stigma on individuals' sexual orientation is greater gender discrimination (Ryan and Wessel 2012).

Antecedents of Workplace Sexual Harassment

Several theories posit that workplace sexual harassment occurs as a reaction to the traditional gender roles threat (Bates et al. 2006); as women gain status and power in the workplace, men harass them as a means of oppression. Bates et al. (2006) also suggest that workplace sexual harassment occurs between actors and targets in an organizational settings, and the act of harassment itself is heavily influenced by the social context.

Actor's Characteristics

Compared to the research on targets' characteristics, researchers have paid less attention to the role of actors' characteristics in understanding workplace sexual harassment (McDonald 2012). Men in higher power positions, such as managers, are frequently reported as actors of workplace sexual harassment. Walker (2014) also showed that former perpetrators engaged in subsequent workplace sexual harassment particularly when they had not been penalized for their previous actions. Actors' characteristics can also moderate the effect of organizational factors on sexual harassment. Dekker and Barling (1998) examined interaction of actors' characteristics with perceptions of company sanctions in predicting the sexual harassment at work. They found that workplace sexual harassment was more likely to occur when individuals with high levels of adversarial sexual beliefs, inappropriate sexual harassment beliefs, and low levels of perspective taking worked in organizations that provided weak rather than strong sanctions for sexual harassment.

Target's Characteristics

The power difference between perpetrators and victims is an important determinant of workplace sexual harassment. Previous studies show that young women and men were more likely to be harassed in the workplace (Chamberlain et al. 2008). Similarly, belonging to a minority group at work is another risk factor for victims. Disabled women, women working in environments dominated by men, homosexual workers, and workers who belonged to a minority race/ethnicity reported that they were victims of workplace sexual harassment more often than workers from the majority group (McDonald 2012). Employees at the intersection of two or more minority identities, such as both gay and a racial minority, were at an even higher risk of workplace sexual harassment than those of one minority identity (McDonald 2012).

Organizational Characteristics

Group level factors explain victimization better than individual factors because workplace sexual harassment affects members of certain groups more than individuals (Quick and McFadyen 2017). Research consistently showed that organizational climate of workplace sexual harassment tolerance was an important factor for predicting the occurrence of harassing behaviors (Willness et al. 2007). A lack of policies and procedures that penalized harassers (McDonald 2012) or a lack of management attention to formal and informal

complaints (i.e., whistle-blowing, Bates et al. 2006) meant harassers could get away with the results of their actions and feel empowered to do it again in the future. Similarly, gender-imbalanced organizations and organizations with high hierarchical structures also contributed to the problems and consequences of workplace sexual harassment (McDonald 2012; Quick and McFadyen 2017).

Outcomes of Workplace Sexual Harassment

Outcomes for Individuals

Experiencing workplace sexual harassment results in a wide array of occupational and mental health problems. In their meta-analysis, Hershcovis and Barling (2010) found that victims of workplace sexual harassment suffered from reduced job satisfaction, co-worker satisfaction, supervisor satisfaction, affective commitment, and psychological well-being, as well as increased turnover intention, job stress, and work withdrawal. Additionally, anxiety, depression, and post-traumatic stress disorder were commonly reported consequences of being a victim of sexual harassment at work (Willness et al. 2007). In another meta-analysis, Sojo et al. (2016) showed that rare but intense forms of workplace sexual harassment, such as sexual coercion and unwanted sexual attention, were as damaging as frequent but less intense forms of workplace sexual harassment, such as gender harassment. Lastly, the negative effects of workplace sexual harassment can go beyond organizational and individual effects to affect functioning in other role domains. For example, Dionisi and Barling (2015) demonstrated that the victims of workplace sexual harassment had difficulties in functioning romantic relationships because of their residual anger feelings from workplace sexual harassment.

Outcomes for Organizations

Workplace sexual harassment can cause damage to organizations both directly and indirectly. The direct costs include legal expenditures spent by organizations to resolve formal disputes around workplace sexual harassment. As sexual harassment is legally forbidden in almost 50 countries (McDonald 2012; Quick and McFadyen 2017), depending on the jurisdiction, organizations can be liable for not taking relevant measures to prevent workplace sexual harassment. The indirect costs of workplace sexual harassment go beyond legal costs to include how organizational functioning may be affected. Reduced employee motivation, morale, and performance can result in significant financial loss for employers. For example, a meta-analysis conducted by Willness et al. (2007) showed that the cost of workplace sexual harassment due to lost productivity was about $22,500 (USD) per person, and this number excluded the costs associated with litigation.

Preventing Workplace Sexual Harassment

Although intervention research aimed at reducing workplace sexual harassment is poorly developed at present, researchers emphasize the role of policy and training could lead to productive changes (e.g., McDonald et al. 2015). In their theoretical discussion, McDonald et al. (2015) examined workplace sexual harassment policies and training, as well as assessment of risk factors, as preventative intervention strategies. Effective policies contain clear statements of what constitutes workplace sexual harassment and articulate the grievance procedures, as well as penalties associated with harassment in a clear way (McDonald et al. 2015). It is not, however, enough to have such a policy. Hunt et al. (2010) underlined that workplace sexual harassment policies were ineffective unless they were enforced with "zero tolerance" principles.

Training is another method frequently used in organizations to reduce workplace sexual harassment. Training programs create awareness of the issue and increase the knowledge of what constitutes workplace sexual harassment. The interdisciplinary review conducted by Roehling and Huang (2018) showed that training could be an productive method in preventing workplace sexual harassment if it had a sound theoretical basis. Additionally, support from management is critical

in workplace sexual harassment training effectiveness (for a full review, please see Roehling and Huang 2018). Finally, workplace sexual harassment training programs can be delivered as a part of incoming employees' orientation. This strategy may be beneficial by delivering the message that workplace sexual harassment is considered a serious offense.

Conclusion

Workplace sexual harassment is a complex problem that affects women and men, minorities, and people from different sexual orientations. Basically, vulnerable workers are at a higher risk of being victims of sexual harassment at work. Workplace sexual harassment has serious consequences for both victims and organizations. Having appropriate policies and training that give a "zero tolerance" message can reduce the likelihood of WSH occurrences in workplaces.

To defeat workplace sexual violence, all members of the organizations must play an active role. Employees must be aware of the existing sexual harassment policies. If no policy exists, they must demand that their employers create, enact, and enforce a sexual harassment policy. Managers must actively monitor for sexual harassment behaviors in their workplaces, collecting data to support whether the policy is effective. They should follow the steps outlined in the policy when they observe others engaging in sexual harassment such as making sexist jokes. Observers of sexual harassment must also be held accountable for reporting the incidents of sexual harassment that they witness. Lastly, open-work culture is key in prevention. Both managers and colleagues must listen to the victims without judgment and encourage employees to report their experiences.

Cross-References

- ▶ Workplace Violence: Sex-Related Crimes
- ▶ Workplace: Hostile Environment

References

Bates, C. A., Bowes-Sperry, L., & O'Leary-Kelly, A. M. (2006). In E. K. Kelloway, J. Barling, & J. J. Hurrell (Eds.), *Handbook of workplace violence* (pp. 381–415). Thousand Oaks: Sage.

Chamberlain, L., Crowley, M., Tope, D., & Hodson, R. (2008). Sexual harassment in organizational context. *Work and Occupations, 35*, 262–295.

Cortina, L. M., & Berdahl, J. L. (2008). Sexual harassment in organizations: A decade of research in review. In J. Barling & C. L. Cooper (Eds.), *The SAGE handbook of organizational behavior: Vol. I. Micro approaches* (pp. 469–497). Thousand Oaks: Sage.

Dekker, I., & Barling, J. (1998). Personal and organizational predictors of workplace sexual harassment of women by men. *Journal of Occupational Health Psychology, 3*(1), 7–18.

Dionisi, A. M., & Barling, J. (2015). Spillover and crossover of sex-based harassment from work to home: Supervisor gender harassment affects romantic relationship functioning via targets' anger. *Journal of Organizational Behavior, 36*(2), 196–215.

Equal Employment Opportunity Commission. (2012, February). Sexual harassment charges EEOC & FEPAs combined: FY 1992 – FY 2011. Washington, DC. Retrieved October 9, 2012, from https://www.eeoc.gov/eeoc/statistics/enforcement/sexual_harassment.cfm

Estrada, A. X., & Berggren, A. W. (2009). Sexual harassment and its impact for women officers and cadets in the Swedish armed forces. *Military Psychology, 21*(2), 162–185.

Fitzgerald, L. F., Drasgow, F., Hulin, C. L., Gelfand, M. J., & Magley, V. J. (1997). Antecedents and consequences of sexual harassment in organizations: A test of an integrated model. *Journal of Applied Psychology, 82*, 578–589.

Hershcovis, M. S., & Barling, J. (2010). Comparing victim attributions and outcomes for workplace aggression and sexual harassment. *Journal of Applied Psychology, 95*(5), 874–887.

Hunt, C. M., Davidson, M. J., Fielden, S. L., & Hoel, H. (2010). Reviewing sexual harassment in the workplace–an intervention model. *Personnel Review*, 39 (5), 655–673.

Kime, P. (2014). Incidents of rape in military much higher than previously reported. Vienna, VA: Military Times.

McDonald, P. (2012). Workplace sexual harassment 30 years on: A review of the literature. *International Journal of Management Reviews, 14*(1), 1–17.

McDonald, P., Charlesworth, S., & Graham, T. (2015). Developing a framework of effective prevention and response strategies in workplace sexual harassment. *Asia Pacific Journal of Human Resources, 53*(1), 41–58.

McLaughlin, H., Uggen, C., & Blackstone, A. (2012). Sexual harassment, workplace authority, and the paradox of power. *American Sociological Review, 77*, 625–647.

Quick, J. C., & McFadyen, M. (2017). Sexual harassment: Have we made any progress?. *Journal of Occupational Health Psychology*, 22(3), 286–289.
Roehling, M. V., & Huang, J. (2018). Sexual harassment training effectiveness: An interdisciplinary review and call for research. *Journal of Organizational Behavior, 39*(2), 134–150.
Ryan, A. M., & Wessel, J. L. (2012). Sexual orientation harassment in the workplace: When do observers intervene? *Journal of Organizational Behavior, 33*(4), 488–509.
Sojo, V. E., Wood, R. E., & Genat, A. E. (2016). Harmful workplace experiences and women's occupational well-being: A meta-analysis. *Psychology of Women Quarterly, 40*(1), 10–40.
Timmerman, G., & Bajema, C. (1999). Sexual harassment in Northwest Europe. *European Journal of Women's Studies, 6*(4), 419–439.
Walker, S. (2014). The automatic activation of sexually harassing beliefs: Past experiences and traits of power. *Academy of Business Journal, 1*, 90–104.
Willness, C. R., Steel, P., & Lee, K. (2007). A meta-analysis of the antecedents and consequences of workplace sexual harassment. *Personnel Psychology, 60*(1), 127–162.

Further Reading

McDonald, P. (2012). Workplace sexual harassment 30 years on: A review of the literature. *International Journal of Management Reviews, 14*(1), 1–17.
Quick, J. C., & McFadyen, M. (2017). Sexual harassment: Have we made any progress? *Journal of Occupational Health Psychology, 22*(3), 286–298.
Willness, C. R., Steel, P., & Lee, K. (2007). A meta-analysis of the antecedents and consequences of workplace sexual harassment. *Personnel Psychology, 60*(1), 127–162.

Workplace Violence: Active Shooter/Terrorist Threats

Kenneth W. O'Donnell
John Jay College of Criminal Justice,
New York, NY, USA

Keywords
Active shooter · Workplace violence · Physical security

Definition

The Federal Bureau of Investigation (FBI 2019) defined an active shooter as one or more individuals actively engaged in killing or attempting to kill people in a populated area (p. 2). This definition excludes shootings that occur in the furtherance of various crimes, such as gang and drug activity.

Introduction

The Federal Bureau of Investigation (FBI 2018, 2019) identified 277 active shooter incidents in the USA from 2000 to 2018, most of which (44%) occurred in commerce locations (see ▶ "Workplace Violence: Past and Current Employees" in this encyclopedia). Approximately one-third of the shooters in business environments were current or former employees or had grievances against the businesses (FBI 2019; Silver et al. 2018). In addition to commerce areas, active shooter incidents have occurred in education environments (24%), healthcare facilities (4%), and government property (10%) which employ teachers, administrators, military, doctors, nurses, and various office staff (Blair and Schweit 2014; FBI 2018, 2019). In the majority of incidents (Silver et al. 2018), the 18-and-older active shooters (who were single, white, men) displayed multiple, disconcerting behaviors usually 25+ months prior to the shooting (56%).

Although the total numbers of incidents and casualties across 19 years (2000–2018) are high, the data shows fluctuation rather than a pattern of steady increase. From 2000 to 2008, there were 67 active shooter incidents resulting in 436 casualties, with a range of 1–14 incidents during this time span (FBI 2018). In contrast, from 2009 to 2016, there were 153 active shooter incidents resulting in 1115 casualties, with a range of 10–26 incidents (FBI 2018). The FBI (2018, 2019) reported the highest number of active shooter incidents for 2017 and 2018, with 30 active shooter incidents resulting in 729 casualties and 27 active shooter incidents resulting in 213 casualties, respectively.

Based on the data presented, it is essential that employees be prepared to address the issue of active shooter threats in their workplaces. The purpose of this entry was to help

organizations to consider an appropriate plan to help employees to prepare, mitigate, respond, and recover when faced with an active shooter situation. All organizations must have active shooter incident preparation in both their emergency management and business continuity plans. While all active shooter incidents cannot be prevented, analysis of active shooter incidents has shown that this violence can be prevented or mitigated through the application of strategies to assess and manage the threat. This entry is organized into the categories of preparation, response, and recovery as a means for presenting employers and managers with the steps that help employees when faced with potential or actual violence at work.

Preparation for Workplace Active Shooter Incidents

Many workplace active shooting incidents can be prevented or mitigated through proper planning and training. Planning for an active shooter incident should be part of an organization's larger emergency response and business continuity plans (see ► "Risk Analysis: National and International Standards" in this encyclopedia). Each plan should consist of a comprehensive scheme to address all aspects of an active shooter incident. Preparation should include training employees and staff in the recognition of potential workplace violence, implementing a broad array of processes for reporting and addressing individuals who are exhibiting the potential to engage in workplace violence, developing physical security measures to maximize workplace protection, and conducting regular drills to prepare staff for an active shooter incident. Organizations need to help their employees recognize when other employees may be prone to commit violence (see ► "Workplace Violence: Factors Contributing and/or Facilitating" in this encyclopedia).

Active shooters have exhibited clusters of externally identifiable behaviors that indicated a potential to engage in violence, initially through oral communication (95%) followed by physical actions (87%) (Silver et al. 2018). When there is a connection between active shooter and the attack site, the recognition and reporting of these clusters of behaviors can serve to prevent an active shooter incident. According to the FBI, there are 21 concerning behaviors demonstrated by past active shooters that had been recognized by others as occurring prior to the attacks (average of 4.7 behaviors). These behaviors have included indications of mental health issues (exhibited in 69% of cases), trouble with interpersonal interactions (exhibited in 59% of cases), and decline in the quality of the shooter's thinking and communications (exhibited in 54% of cases). Furthermore, 56% of active shooters exhibited what the study called "leakage," which was the shooter communicating with a third party their intent to harm someone. Other behaviors commonly observed in active shooters were poor work performance (46%), threats/confrontations (35%), anger (33%), and physical aggression (33%) (Silver et al. 2018).

As part of an organization's comprehensive plan to address an active shooter incident, employees should be trained to recognize clusters of behaviors indicative of an individual's likeliness to engage in violence and also be encouraged to report these behaviors to management. The FBI study on active shooters referenced above revealed in 40% of the cases, coworkers observed concerning behaviors of the active shooter prior to the attack (Silver et al. 2018). However, the employees either did not feel comfortable or did not believe they had a process to report these indicators to management. Employees may be reluctant to report the concerning behavior of coworkers because they do not want to be perceived to be undermining their peers. They often will wait until they are certain that an individual is serious about engaging in violence before reporting the individual. This is often too late. In order to maximize the prevention of active shooter attacks, organizations should create an environment where employees feel comfortable reporting potential indicators that an individual may engage in violence.

The creation of multiple pathways through which employees can report a colleague's behavior indicating a potential to engage in violence may increase the likelihood of obtaining this information in a timely manner. An environment should be created where employees feel

comfortable reporting concerning behavior of a coworker directly to a supervisor, knowing this information will be handled safely and discreetly. Workers may also be encouraged to relay information regarding suspicious behavior to their human resource or security departments. Some employees may not feel comfortable reporting suspicious behavior directly to another person. Therefore, organizations should have a process whereby employees can communicate their concern via e-mail or text message. Organizations can also employ drop boxes and tip hotlines to allow employees to report suspicious behavior while also maintaining their anonymity (Romano et al. 2011).

Physical Security in a Workplace

Proper facility management is instrumental in preventing or mitigating the effects of an active shooter (see ▶ "Physical Security: Best Practices" in this encyclopedia). The goal of physical security is to limit the ability of a shooter to access a site. Facilities managers should conduct a security assessment to determine the facility's vulnerability to an active shooter attack (see ▶ "Physical Security: Methods and Practices" in this encyclopedia). As part of this assessment, facilities managers should identify multiple evacuation routes in the event of an attack. These evacuation routes should be posted in conspicuous locations in a facility. This preparation should establish evacuation routes and procedures for individuals with special needs and disabilities (Alvarez et al. 2012).

Access controls, such as keys and security pass codes, should be instituted by management to limit access to a location to those permitted to be there. These credential-based systems can provide accurate accounting of those inside a facility. Site security, such as ensuring external doors and windows to a facility are locked from the outside, should be employed to further limit access to a facility. Ideally, closed-circuit television systems that provide views of an entire facility and can be accessed from a central command station should be installed (Alvarez et al. 2012).

In order to maximize communication in the event of an emergency, organizations should install a communications infrastructure that allows for facility-wide messaging. If the facility has elevators, the organization should install an elevator system that may be controlled or locked down from a central command station. An individual with knowledge of a facility's security procedure and floor plan should be designated to serve as a liaison with police and emergency responders in the event of an attack. Organizations should establish a central command station from which all security issues inside a facility can be addressed. If a facility has security guards, their patrols and patterns of operation should be varied to ensure that potential active shooters cannot circumvent a routine patrol. In order to maximize security, organizations should limit access to blueprints, floor plans, and other documents containing sensitive security information, but should make these documents available to law enforcement agents responding to an emergency (Alvarez et al. 2012).

Employee Training and Drills

Active shooter incidents should be addressed as part of an organization's comprehensive planning for workplace emergencies. Employee training for active shooter incidents should include familiarizing all employees with their expected response to an active shooter, the floor plan of the building, potential exits, and potential assembly areas outside the building for employees to regroup after evacuation during an incident. Ideally, this training will include both classroom training and drills where employees will practice their response to an active shooter and their evacuation from the facility. Outside organizations can be employed to conduct realistic active shooter drills to maximize employee training in the response to such incidents (Alvarez et al. 2012).

Response to an Active Shooter Incident

Both law enforcement personnel and private citizens have the potential to affect the outcome of an active shooter incident based upon their response. The first task of law enforcement when responding to an active shooter incident is to end the threat presented by the shooter in order to

reduce the casualty rate. Officers may have to pass injured victims as they proceed to confront the attacker. Once the shooter has been neutralized and the threat ended, the responders can address the injured and wounded. When arriving at the scene, responding officers usually do not know who the shooter is or whether he or she is acting alone. Therefore, employees must be sure to keep their hands empty and visible at all times. For their own safety, employees should follow the commands of the police and not run at them as officers enter the building or the room where the employee is located (Department of Homeland Security, DHS 2008).

Employees' responses to an active shooter in the workplace can be divided into three options – evacuate, hide, or fight – which they should do in that order (Alvarez et al. 2012). If there is an active shooter in the workplace, the primary response from employees should be to flee the scene if it is safe to do so. As their personal safety is of paramount concern, employees should not take the time to gather personal belongings. Instead they should leave all belongings behind and immediately flee. If they may safely do so, employees should warn others of the active shooter and instruct them to flee as well. After an employee has arrived in an area where they are safe, they should call 911 and notify the authorities of the shooter. 911 callers should describe each shooter in as much detail as possible, explain their locations, and describe the weapons the shooter may possess (DHS 2008).

When employees cannot safely flee the location, they should attempt to find a place to hide. Employees should hide in a location out of the shooter's view and stay as quiet as possible. They should silence all electronic devices and ensure they won't vibrate. They should also lock the doors and then barricade them with furniture, if possible. Employees should close any blinds or window shades and turn off the lights. The darkening of a room provides a tactical advantage for the employee as the shooter will have a difficult time seeing in the room from the outside and, if the shooter were to enter the room, the employee may have a momentary tactical advantage as the shooter's eyes have to adjust to the darkness (DHS 2008).

Fighting is a last resort in an active shooter scenario. When employees are in immediate danger and are unable to flee or hide, they should take every step to defend themselves to end the active shooter threat (DHS 2008). When engaging an attacker, employees should commit to their actions and act aggressively. They should remember that their attacker is trying to kill them and that they must aggressively act to end this threat to their lives. Whenever possible, employees should act together to ambush the shooter with makeshift weapons such as chairs, fire extinguishers, scissors, or whatever other weapons of opportunity may present themselves (DHS 2008).

Recovery from an Active Shooter Incident

The recovery process from an active shooter incident begins as soon as the emergency has ended. This process can be divided into initial and long-term recovery phases. The ultimate purpose of this process is to assist personnel in recovery and to restore organizations to their full functionality as soon as possible. The initial recovery process focuses on reestablishing safety and mitigating the effects of the incident. This process should begin immediately after an active shooter incident is completed. The establishment of active shooter response procedures and the conducting of drills as part of an organization's emergency planning process will ensure prompt and efficient implementation of the short-term recovery process (DHS 2017).

One of the first response tasks for an active shooter incident is to evacuate personnel to a safe area in an orderly fashion. As part of an organization's emergency planning, assembly areas for fire drills and other emergency incidents should be pre-designated. Staff and management should be trained in the location of these areas and the proper evacuation routes. Once evacuees have arrived at assembly areas, leadership should account for all evacuees and inform authorities

of those accounted for. Both management and the authorities should use the assembly area as a venue to address employees and inform them of updates and further steps in the recovery process. In order to ensure safety and accountability, evacuees should be instructed not to leave the assembly area until after they have been informed that it is safe to do so by authorities (DHS 2017). Management should ensure that individuals who have been injured or wounded during an incident are provided with emergency medical care from first responders at the assembly area. They should also ensure that individuals who require a greater degree of care than can be provided at the assembly area are transported to medical facilities (DHS 2017).

Organizational Crisis Communication and Media Response

It is imperative that organizations convey accurate and timely information regarding an active shooter incident (see ▶ "Emergency Management: Crisis communication" in this encyclopedia). As part of the active shooter response plan, organizations should ensure that crisis communication plans are in place and that there is a designated spokesperson to conduct all communications regarding the incident. The spokesperson chosen to conduct crisis communication should be well trained and briefed to provide responses to stakeholders, media, employees, and the public. Crisis communication should be closely coordinated with law enforcement to ensure it does not compromise the investigation or endanger safety (Stowell 2017). This communication should include information regarding the incident, contact information for emergency assistance, and other information that will help facilitate recovery. Employees who are not present at the scene of the incident should be provided with instructions regarding whether and when they are expected to report to work. As soon as possible, evacuees' families and friends should be told about their whereabouts and status. An organization's websites and social media accounts are effective means for conveying information. News media can also be utilized to communicate with the public (DHS 2017).

Reunification

Reunification of evacuees and survivors with their families and friends is an important aspect of the initial recovery process. Management should be prepared to accommodate the various needs of family members and friends and should implement a process to accommodate those who may rush to an incident scene. Friends and family members of survivors should be informed of assembly area locations as well as provided with estimates for when they can reunite with affected employees. In order to facilitate swift reunification, management should consider providing friends and family members with transportation to hospitals where survivors may have been taken (Department of Justice 2015).

Crisis Support in the Aftermath of an Incident

Management should consider setting up a Family Assistance Center (FAC) at the assembly areas if such assistance would be helpful in meeting the needs of affected employees. An FAC can be a formal or informal process to provide a wide array of assistance to survivors immediately after an incident. Assistance may include providing information about survivors relocated to hospitals or other assembly areas and the arranging for the reunification of survivors with their families and friends. FACs can also provide other necessary services such as temporary housing and meals and the coordination of legal and social services. A FAC can offer a confidential environment for families and friends of deceased victims to grieve in privacy (DHS 2017).

Retrieval of Personal Belongings

Procedures for workplace response to an active shooter incident emphasize that, if possible, employees should leave the scene immediately without taking time to gather personal belongings. Therefore, after the resolution of most incidents, many evacuees will want to retrieve personal

belongings left behind at the scene. Management should coordinate with law enforcement to set up a process for reclaiming personal property or notifying employees which items may be needed as evidence in the criminal investigation and legal proceedings (DHS 2017).

Long-Term Recovery

The objective of long-term recovery is to help employees return to a sense of normality and to return an organization to full functionality after an active shooter incident. The process of long-term recovery depends upon the specific organization as well as the circumstances of the active shooter incident (DHS 2017). Recovery should include employee assistance programs, grief counseling, reopening of the facility, holding memorials and anniversaries of the incident, and preparing employees for civil and criminal proceedings involving the active shooter incident.

Depending on the specifics of the active shooter attack, and the employee's role in an incident, individuals may suffer from an array of physical, psychological, and financial woes. One way that an organization can prepare to address the broad array of challenges that survivor employees may face is by establishing an employee assistance program (EAP). An EAP is a program that assists employees in addressing personal and work-related problems. This type of program can be beneficial in a myriad of ways to employees and may serve to facilitate the long-term recovery process. For example, an EAP can provide employees with access to grief counseling and assist with workers' compensation claims and other types of financial assistance. If an active shooter incident has resulted in injuries or deaths, an EAP can assist the affected individuals in applying for compensation for their medical expenses (DHS 2017).

Smaller organizations that do not have the resources of a large entity should consider utilizing outside community resources in order to provide this type of assistance. Thorough emergency planning should include exploring the available community resources that may assist in recovery (Stowell 2017).

The psychological impact of an active shooter incident on individuals can vary greatly for each person affected. Grief counseling can be an important tool to assist the recovery process for a broad spectrum of individuals impacted by an incident including survivors, their families, and friends. Proper planning for workplace emergencies should ensure that victims have access to grief counseling if needed (DHS2017).

Most organizations will seek to reopen their facilities as soon as possible after an active shooter incident has occurred. Proper emergency planning for an organization should include a business continuity plan to address the most efficient means to reestablish full operations as quickly as possible. This plan may include a variety of provisions that may be applicable depending on the specifics of an incident, including establishing alternate work locations and employing temporary staff. In seeking to reestablish operations, organizations should be aware that individuals recover from traumatic events at varying rates. Some individuals will recover quickly and return to work within days. Other will require more time or will not return to work at all. As much as possible, organizations should seek to accommodate the recovery process for employees. Organizations that have suffered an active shooter event should also conduct an after-action report to evaluate the response to the incident. This type of analysis can be helpful for both the affected organization and other organizations to establish best practices for active shooter events (DHS 2017).

Another way to aid in the process of grief is to hold anniversaries and memorial services to assist survivors and their friends and families address their traumatic experience and progress on the road to recovery. They can serve as an opportunity for survivors to reconnect with former coworkers. Organizations may consider facilitating memorial services as a way to help employees and their friends and families in the long-term recovery process (DHS 2017).

Finally, it is important to help employees with the legal aspects of the active shooting incident,

including both criminal and civil litigation. Comprehensive planning for active shooter incidents should include training for legal staff on the various civil and criminal law issues that may arise from such an attack. Management should ensure that the legal staff is prepared for requests for cooperation from authorities investigating and prosecuting criminal cases. The organization must also be aware that they may be the subject of various legal processes as part of a criminal investigation including subpoenas and search warrants. Furthermore, legal staff should be prepared to address potential civil litigation related to the incident (DHS 2017).

Organizations should be aware that employees may have to testify in various criminal or civil proceedings related to the active shooter incident as well as engage in preparation for their testimony. As part of their planning, management should consider a leave policy that accounts for employee absence during judicial proceedings. Furthermore, as part of the training for their response to an active shooter incident, employees should be made aware that they may be called to testify in various judicial proceedings (DHS 2017).

Conclusion

The number of active shooter incidents per year has more than doubled in the past 8 years when compared to the previous 7 years. A significant number of these incidents occur in a workplace. Active shooter incidents enact a toll that transcends the immediate numbers of those killed or wounded and can result in significant economic, psychological, and social costs. While all active shooter incidents cannot be prevented, proper preparation, response, and recovery can serve to prevent many attacks and mitigate the impact of those that do occur.

Cross-References

- ▶ Emergency Management: Crisis Communication
- ▶ Physical Security: Best Practices
- ▶ Physical Security: Methods and Practices
- ▶ Workplace Violence: Factors Contributing and/or Facilitating
- ▶ Workplace Violence: Past and Current Employees

References

Alvarez, R., Andersen, J., Biddle, C., Clark, S., Cotter, J., Merola, R.,... Levine, E. (2012). *Active shooter: Recommendations and analysis for risk mitigation*. New York: Police Department. Available at: https://www.hsdl.org/?view&did=11489

Blair, J. P., & Schweit, K. W. (2014). *A study of active shooter incidents, 2000–2013*. Washington, DC: Texas State University and Federal Bureau of Investigation, U.S. Department of Justice. Available at: https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1.pdf/view

Department of Homeland Security. (2008). Active shooter how to respond. Available at: https://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf

Department of Homeland Security. (2017). Active shooter recovery guide. Retrieved from: https://www.dhs.gov/sites/default/files/publications/active-shooter-recovery-guide-08-08-2017-508.pdf

Department of Justice, Office of Victims of Crime. (2015). Partnerships and planning checklist. Available at https://www.ovc.gov/pubs/mvt-toolkit/PartnershipsPlanningChecklist.pdf

Federal Bureau of Investigation. (2018). Quick look: 250 active shooter incidents in the United States from 2000 to 2017. Available at: https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents-graphics

Federal Bureau of Investigation. (2019). Active shooter incidents in the United States in 2018. Available at: https://www.fbi.gov/file-repository/active-shooter-incidents-in-the-us-2018-041019.pdf/view

Romano, S., Levi-Minzi, M., Rugala E., & Van Hasselt, V. (2011). Workplace violence prevention. Available at: https://leb.fbi.gov/articles/featured-articles/workplace-violence-prevention-readiness-and-response

Silver, J., Simons, A., & Craun, S. (2018). *A study of pre-attack behaviors of active shooters in the United States between 2000 and 2013*. Available at: https://www.fbi.gov/file-repository/pre-attack-behaviors-of-active-shooters-in-us-2000-2013.pdf/view

Spanheimer, J. (2018, Dec. 5). Active shooter response: Developing a tactical playbook. *Police Chief online*. Available at: http://www.policechiefmagazine.org/active-shooter-response-playbook/

Stowell, H. G. (2017, May). After an active shooter. *Security Management, 61*(4). Available at: https://sm.asisonline.org/Pages/After-an-Active-Shooter.aspx.

Further Reading

Federal Bureau of Investigation. (2017). Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks. Available at: https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view

Modell, D. A. (2013). The psychology of the active killer. *Law Enforcement Executive Forum, 13*(4), 1–9. Retrieved from https://iletsbeiforumjournal.com/images/Issues/FreeIssues/LEEF_13.4_December_2013.pdf.

Schweit, K. W. (2013, May 07). Addressing the problem of the active shooter. Retrieved from https://leb.fbi.gov/articles/featured-articles/addressing-the-problem-of-the-active-shooter

Workplace Violence: Assault

Duygu Biricik Gulseren and E. Kevin Kelloway
Department of Psychology, Saint Mary's University, Halifax, NS, Canada

Keywords

Physical assault · Workplace violence · Homicide · Nonfatal workplace assault

Definition

Workplace assault refers to physically violent acts targeted at people at work or on duty with the intention of hurting them (LeBlanc and Kelloway 2002).

Introduction

For teachers, nurses, police, and many others, "bites, cuts, bruises are part of the job" ("5 most violent workplaces in Nova Scotia" 2014). Although this potential hazard may have been considered for many years as an unpreventable aspect of their employment, employees and their employers are now seeking ways to prevent workplace assaults. This entry aims to define, describe, and explain workplace assault.

Definitions of workplace assault used in different jurisdictions, such as by the National Institute for Occupational Safety and Health (NIOSH), includes threats of violent acts within the domain of workplace assault as well as physical violent acts themselves (Jenkins 1996). Some theorists have also suggested that assault can also be psychological or verbal (e.g., Gillespie et al. 2010); however, this view is increasingly rare. For example, Schat et al. (2006) operational definition of workplace assault included four categories of behaviors: (1) pushing, grabbing, and slapping; (2) kicking, biting, and hitting; (3) hitting or physically attempting to hit with an object; and (4) attacking with a weapon including a knife.

The lack of a consensus in the definition of workplace assault is a problem for three reasons. First, studies reporting prevalence rates are incomparable if they are based on different conceptual and operational definition of workplace assault. Second, victims of workplace assaults may have difficulty in identifying the problem; therefore, they may underreport incidents. Third, effective prevention strategies may differ depending on the adopted definition. For example, policies targeted to prevent verbal assault may be ineffective for situations where the problem of assault was conceptualized as purely physical acts. The best solution currently available is for researchers to use an operational definition (e.g., see Schat et al. 2006, above) in their reports which will allow everyone to understand what behaviors were included. In order to understand the complexity of workplace assault, the rest of the chapter will describe the literature regarding prevalence, sources, antecedents, outcomes, mediators, moderators, and prevention.

Prevalence of Workplace Assault

Nationally representative studies across the world report the incident rate of workplace assaults as 8% in Denmark (Hogh et al. 2003), 6% in the United States (Schat et al. 2006), 4% in Finland (Salminen 1997), and 1.5% in the United Kingdom (Cookson and Buckley 2012). Differences in national prevalence rates may reflect cultural features but may also reflect differences in sampling strategies and/or definitions of assault. For

example, Francis and Kelloway (2007) adopted the NIOSH's (1996) definition, which includes threats of violence and reported that 21% of their sample reported being victimized. Schat et al. (2006) excluded threats of violence and implemented a more rigorous sampling plan resulting in a prevalence rate of 6%.

Although workplace assault has a low base rate for the general population, workers belonging to specific occupational groups are exposed to assault more often than are others. Employees in protective services, such as police, military, and correctional workers, are at the highest risk (Schonfeld and Chang 2017). For these workers, violence is an expected part of the job as dealing with violent situations is literally part of the job description, and workers are typically provided with specific training and weapons in order to defend themselves and to stop potential assaults. However, the next highest risk group comprises individuals in occupations that work with the public to provide a service, such as nurses, teachers, retail workers, and bus drivers. In contrast to workers in protective services, service workers are rarely provided with specific training or means to defend themselves from assault.

LeBlanc and Kelloway (2002) suggested that occupational differences in the prevalence of assault were a function of specific occupational risk factors. They showed that such occupational risk factors (e.g., working alone, at night, around valuables, caring for other, or being the position of denying a service or enforcing rules) predicted workers' experience of violent assault and psychological aggression across occupations. In doing so, they demonstrated that the risk of violence was a foreseeable aspect of the job.

Sources of Workplace Assault

The United States Department of Labor and Occupational Safety and Health Administration's (OSHA 1996) classification of general workplace violence is based on the source and thus also applies to the topic of assault. The perpetrator of the assault can be (1) a stranger with a criminal intent such as a robber (i.e., type I violence), (2) a customer or client (i.e., type II violence), (3) a colleague or a past employee of the victim's employer (i.e., type III violence), or (4) someone from the victim's personal life, such as a family member (i.e., type IV violence). This classification is important because public-initiated and organization-initiated assaults have different outcomes (LeBlanc and Kelloway 2002). Type 1 and Type 2 public-initiated assaults are harder to prevent than Types 3 and 4 organizational-initiated assaults. Specifically, organizational policies developed to reduce or stop workplace assault perpetrated by insiders, but they are not capable, per se, of controlling the behaviors of customers and strangers.

Antecedents of Workplace Assault

Victim Characteristics

Victims of workplace assault share few demographic characteristics. Schat et al. (2006) showed that workers who are between 26 and 40 years old were more likely to be assaulted at work than those younger or older than this age range. Piquero et al. (2013) systematic review showed that, although male workers are more likely than female workers to be victims of a workplace assault, women reported assault incidents to the formal authorities more than men. Hogh and colleagues (2003) also noted that former victims of workplace assault were at risk for being assaulted again, perhaps because they did not report the initial incident. They attributed the positive relationship between past and future victimization to the worker's continuing tenure in a high-risk occupation.

Perpetrator Characteristics

Although the majority of the studies on workplace assault examined risk factors, studies have identified common characteristics across perpetrators. These included a history of violence, aggression and substance abuse, unstable self-esteem, negative affect, and trait anger (Barling et al. 2009). Although there is a small effect, some perpetrators suffer from mental illnesses (Barling et al. 2009). Lastly, client/customer stress due to an unfavorable interaction with the

worker or perpetrator's perceived aggression was also found to trigger workplace assaults (Piquero et al. 2013).

Work Characteristics

In general, dealing with the public, working in impoverished locations, handling money, or working in night shifts were primary risk factors for being a victim of an assault at work (Piquero et al. 2013; Schonfeld and Chang 2017). Studies conducted in the healthcare settings showed that working in the stressful environments, such as emergency rooms, psychiatric units, and addiction treatment facilities, increased the likelihood of being assaulted at work. LeBlanc and Kelloway (2002) identified 22 risk factors for violence. Their results showed that workers who handled weapons, exercised physical control over others, and dealt with individuals under medication were the most at risk for public-initiated assault (for the full list of risk factors, please review LeBlanc and Kelloway 2002). Lastly, working in stressful environments was associated with being a target of a workplace assault (Piquero et al. 2013).

Outcomes, Mediators, and Moderators of Workplace Assault

Although the prevalence rates of workplace assault are the lowest among all types of workplace aggression and violence, they have detrimental consequences on workers and their employers. These outcomes can be organized into two major categories: (1) health-related outcomes and (2) organizational outcomes. Health-related outcomes include impaired physical and psychological well-being indicators, such as increased somatic health complaints, burnout, depression, and low self-esteem (e.g., Hurrell et al. 1996; Mueller and Tschan 2011; Schat and Kelloway 2003). Organizational outcomes include undesirable consequences, such as financial burden to the organization, negative job-related affect, and turnover (Piquero et al. 2013; Schat and Kelloway 2003). Fear of future violence mediates the relationship between assault and its negative outcomes (Rogers and Kelloway 1997). Additionally, organizational support moderates the relationship between workplace violence and its negative outcomes such as that as organizational support increases, the link becomes weaker (Schat and Kelloway 2003).

Preventing Workplace Assault

The majority of intervention studies on workplace assault have been conducted in healthcare and retail settings. Workplace interventions aiming to prevent workplace violence are categorized in three groups: (1) environmental interventions, (2) organizational and administrative interventions, and (3) behavioral/interpersonal interventions. Environmental interventions, such as lighting the entrances or electronically controlled cash drop boxes, aim at changing the physical environment so that perpetrators are discouraged to attempt to assault. Organizational and administrative interventions involve policies and practices to protect workers from possible assaults. For example, many organizations have "zero tolerance policy" for workplace violence or harassment. This policy not only gives the message that assault is unwelcome in that workplace but also warns potential perpetrators about the consequences of their actions. Lastly, behavioral or interpersonal interventions include training programs to educate workers so that they know how to recognize and deal with assault. For example, conflict de-escalation techniques training programs teach employees how to recognize the cues of a potential assault and how to avoid it by taking preventative actions such as calming down the potential perpetrator. Studies have shown that environmental interventions are the most effective for preventing workplace assaults, but not all of research implement rigorous designs (Wassell 2009).

Conclusion

Workplace assault referring to a physical attack at work is a specific type of workplace violence. Compared to the verbal and psychological violence and aggression, workplace assaults have a lower occurrence rate. However, the

prevalence of this problem is highest in occupations involving those in protective or service-related employment. Assaulted employees suffer from ill health and produce poor organizational outcomes, mostly because of the fear of future violence against them. Based on the victim, perpetrator, and workplace characteristics, workplace assaults can be predicted.

There are several different ways to prevent workplace assaults, such as establishing environmental control methods, developing assault related policies, and training employees for possible assault scenarios. As a starting point, organizations should identify the primary sources of assault in their workplaces because the effectiveness of action can differ depending on the type of perpetrator (organizational/insider or public/outsider). There are several different types of workplace interventions on this topic. Among the intervention strategies, environmental control is known as the most effective in preventing workplace assaults by public perpetrators. In such cases, organizational decision-makers can consider redesigning their offices to reduce physical contact between their employees and the public. If Type III or Type IV violence is more common than the others, zero-tolerance policies and respectful work environment training have been effective for prevention.

Organizations must keep a record of incidents of assault that have occurred in their facilities. This is important, not only to identify the common sources of assault but also the employee and work characteristics that contribute to assault risk factors. Lastly, creating an open culture is essential to improve safety in the workplace. Employees should be encouraged to share their opinions about the effectiveness of the measures that have already been taken and to suggest what else they would like to see implemented to increase safety.

Cross-References

- ▶ Workplace Violence: Active Shooter/Terrorist Threats
- ▶ Workplace Violence: Factors Contributing and/or Facilitating
- ▶ Workplace Violence: Intimate Partner Violence

References

5 most violent workplaces in Nova Scotia. (2014, February 19). *Canadian Broadcasting Channel News*. Retrieved from https://www.cbc.ca/news/canada/nova-scotia/5-most-violent-workplaces-in-nova-scotia-1.2544020

Barling, J., Dupré, K. E., & Kelloway, E. K. (2009). Predicting workplace aggression and violence. *Annual Review of Psychology, 60*, 671–692.

Cookson, H., & Buckley, P. (2012). *Violence at work: Findings from the 2010/11 British Crime Survey*. London: Health and Safety Executive.

Francis, L., & Kelloway, E. K. (2007). *The Nova Scotia workplace stress survey*. Halifax: Saint Mary's University.

Gillespie, G. L., Gates, D. M., Miller, M., & Howard, P. K. (2010). Workplace violence in healthcare settings: Risk factors and protective strategies. *Rehabilitation Nursing, 35*(5), 177–184.

Hogh, A., Borg, V., & Mikkelsen, K. L. (2003). Work-related violence as a predictor of fatigue: A 5-year follow-up of the Danish Work Environment Cohort Study. *Work and Stress, 17*, 182–194.

Hurrell, J. J., Jr., Worthington, K. A., & Driscoll, R. J. (1996). Job stress, gender, and workplace violence: Analysis of assault experiences of state employees. In G. R. VandenBos & E. Q. Bulatao (Eds.), *Violence on the job: Identifying risks and developing solutions* (pp. 163–170). Washington, DC: American Psychological Association.

Jenkins, L. (1996). *Violence in the workplace: Risk factors and prevention strategies*. US Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, Division of Safety Research. Washington DC.

LeBlanc, M. M., & Kelloway, E. K. (2002). Predictors and outcomes of workplace violence and aggression. *Journal of Applied Psychology, 87*(3), 444–453.

Mueller, S., & Tschan, F. (2011). Consequences of client-initiated workplace violence: The role of fear and perceived prevention. *Journal of Occupational Health Psychology, 16*(2), 217–229.

National Institute for Occupational Safety and Health. (1996). *Violence in the workplace* Retrieved August 30, 2000, from http://www.cdc.gov/niosh/violphs.htm.

Piquero, N. L., Piquero, A. R., Craig, J. M., & Clipper, S. J. (2013). Assessing research on workplace violence, 2000–2012. *Aggression and Violent Behavior, 18*(3), 383–394.

Rogers, K. A., & Kelloway, E. K. (1997). Violence at work: Personal and organizational outcomes. *Journal of Occupational Health Psychology, 2*(1), 63–71.

Salminen, S. (1997). Violence in the workplaces in Finland. *Journal of Safety Research, 28*, 123–131.

Schat, A. C., & Kelloway, E. K. (2003). Reducing the adverse consequences of workplace aggression and violence: The buffering effects of organizational support. *Journal of Occupational Health Psychology, 8*(2), 110–122.

Schat, A., Frone, M. R., & Kelloway, E. K. (2006). Prevalence of workplace aggression in the U.S. workforce. In J. J. Hurrell, J. Barling, & E. K. Kelloway (Eds.), *Handbook of workplace violence* (pp. 47–89). Thousand Oaks: Sage.

Schonfeld, I. S., & Chang, C. H. (2017). *Occupational health psychology*. New York: Springer Publishing Company.

U.S. Department of Labor & Occupational Safety and Health Administration. (1996). *Guidelines for preventing workplace violence for healthcare and social service workers* (No. OSHA 3148). Washington, DC: U.S. Department of Labor & Occupational Safety and Health Administration.

Wassell, J. T. (2009). Workplace violence intervention effectiveness: A systematic literature review. *Safety Science, 47*(8), 1049–1055.

Further Reading

Jenkins, L. (1996). *Violence in the workplace: Risk factors and prevention strategies*. US Department of Health and Human Services, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health, Division of Safety Research.

Schat, A., Frone, M. R., & Kelloway, E. K. (2006). Prevalence of workplace aggression in the U.S. workforce. In J. J. Hurrell, J. Barling, & E. K. Kelloway (Eds.), *Handbook of workplace violence* (pp. 47–89). Thousand Oaks: Sage.

Wassell, J. T. (2009). Workplace violence intervention effectiveness: A systematic literature review. *Safety Science, 47*(8), 1049–1055.

Workplace Violence: Factors Contributing and/or Facilitating

Lisa van Reemst
Department of Criminology, Erasmus School of Law, Erasmus University Rotterdam, Rotterdam, The Netherlands

Keywords

Workplace aggression · Contributing factors · Correlates

Definition

Workplace violence is "behaviour that a target wants to avoid, takes place in a work-related situation, and is potentially physically or psychologically damaging to the target" (Schat and Frone 2011).

Introduction

Workplace violence is considered a problem in many countries and among many occupational groups. Workplace violence refers to acts of aggression toward employees in a work-related context. Acts of aggression can, for example, include hitting, kicking, threatening, calling names, and bullying. The context of work can be the work location and during work hours but also outside these locations and hours, as long as there is a connection with work, such as a work relationship between persons. Workplace violence can occur in many variations. Incidents differ broadly in the occupational group it concerns, the type of workplace violence, and the type of relationship between victim and offender. First, workplace violence concerns all occupational groups, such as people at the office, service providers, and law enforcement employees. Second, regarding the type of workplace violence, workplace aggression can be physical (such as hitting and kicking) and psychological (such as calling names). Threats could be considered a form of psychological aggression, but some scholars consider this a separate type. In addition, specific forms of aggression are studied, such as sexual aggression, which can be psychological and physical. Third, the relationship between victim and offender can differ. Overall, there can be workplace violence between colleagues, between supervisor and subordinates, and between employee and citizen. This can be referred to as internal workplace aggression (initiated by people inside the work organization) or external workplace aggression (initiated by people outside the work organization). Often these variations co-occur. For example, looking at law enforcement officers (occupational group), they are most often exposed to external workplace violence (relationship between victim and offender), and while psychological aggression

is more common overall, they are more often exposed to physical violence than other occupational groups (type of aggression) (Van Reemst and Fischer 2016).

It is clear that workplace violence is, to some extent, not random (Barling et al. 2009). This means that there are characteristics that are related to workplace violence and that may contribute or facilitate workplace violence. This chapter will provide an overview of factors contributing to and facilitating workplace violence. These factors can be aspects of offender, victim, or context, as one can look at who the offenders are, who the victims are, or in which contexts workplace violence occurs. It is important to note that research about workplace violence is often based on a single survey, which means that is difficult to establish to what extent factors are actually facilitating or contributing to workplace violence, or more so a consequence of having experienced violence. It is thus important to interpret the results that will be described in this chapter with that in mind. The following paragraphs will first discuss offender characteristics contributing to workplace violence, victim characteristics, and then context characteristics. Each type of factor will be introduced by a real-world case of aggression against public service employees. Finally, possible variations in factors contributing to workplace violence will be discussed and a conclusion will be drawn.

Offender Factors

> A man who is caught during the day urinating in public. He runs away and spits the police officer who chases him in his face. When the officer catches him up, the man hits the officer with a fist against his jaw. After his arrest, the man bites in the hand of another police officer. (Bergman et al. 2013).

Offender characteristics can be related to workplace violence. Some people are more likely to offend than others, which, in general, is explained by being more driven by hostile or instrumental motives (reactive or proactive aggression) or by learning from previous social experiences (Penney et al. 2017). For example, in the described case, the man could, in general, have hostile tendencies or have the instrumental goal to escape from the police. Characteristics related to conducting workplace violence include sociodemographic, work, and psychological characteristics of this person. Regarding sociodemographic characteristics, aggressiveness in the workplace seems to be more often conducted by males than females. However, support for other associations with sociodemographic characteristics, such as with age, race, or socioeconomic status, is limited (Barling et al. 2009).

In addition, work characteristics could be factors related to conducting workplace violence. Both job and social stressors seem related to enacting workplace violence (Penney et al. 2017). Job stressors, for example, include conditions that interfere with task performance, such as insufficient time or assistance. Social stressors, for example, include perceived injustice (Penney et al. 2017). People who in general experience more job stressors and social stressors are more likely to enact workplace violence, possibly as a response to these stressors.

Furthermore, general psychological characteristics such as personality traits could be factors related to conducting workplace violence. Employees who have more propensity to experience negative affect, such as anger and sadness, seem more likely to conduct workplace (Barling et al. 2009, p. 676). In addition, employees with more trait anger and aggressiveness seem more likely to conduct workplace violence. Furthermore, employees with a history of aggression are more likely to conduct workplace violence again (Barling et al. 2009, p. 676), which could be related to described traits or social learning. Regarding offenders who are not employees, being under the influence of alcohol, drugs, or medicine seems to be related to offending an employee as a citizen (LeBlanc and Kelloway 2002). Offender characteristics, including sociodemographic, work, and psychological characteristics, are thus a group of factors that seem to contribute to workplace violence, particularly by

general tendencies and motivation to perform violence.

Victim Factors

> A young woman finds a man who is unconscious in the street and she calls an ambulance. It arrives quickly, but when the ambulance nurse succeeds in bringing the man to some level of consciousness, the nurse receives a head-butt. (Bergman et al. 2013).

Victim characteristics, in this case, characteristics of employees, can be related to exposure to workplace violence, due to the extent that possible victims are in contact with motivated offenders and lack guardianship and are suitable to become a victim (Cohen and Felson 1979). For example, employees could be more likely to be exposed to workplace violence if they are more often in contact with other people or, more specifically, people who tend to offend. Furthermore, employees could be more likely to be exposed to workplace violence if they lack safety precautions, such as social control or organizational policies, that limit workplace aggression. In addition to the situational opportunity to become a victim, there could also be a personal vulnerability to become a victim. For example, employees could be more likely to be exposed to workplace violence because they have characteristics that motivate others (more) to offend. This idea is based on the victim precipitation theory (Wolfgang 1958) which suggests that victims contribute to their own victimization. This theory has been criticized for blaming the victim, in this case the employee, but personal characteristics of victims could still be related, as has been shown in multiple studies. More specifically, some employees could act in ways, for example, violating norms or threatening others' identities, that, knowingly or unknowingly, results in being targeted (Aquino and Thau 2009, p. 723). Although the described case does not clarify the reason behind the head-butt, it is possible that the nurse, probably unknowingly, influenced this behavior of the patient. Based on studies about victim characteristics, three types of victim characteristics that may contribute to workplace violence will be distinguished: sociodemographic, work, and psychological characteristics.

Sociodemographic characteristics such as gender and age could be factors related to exposure to workplace violence. Overall, males seem to be more often exposed to aggression than females, and younger employees seem to be more often exposed to aggression at work than older employees. However, these are only small differences (according to a meta-analysis: Bowling and Beehr 2006). In addition, these are likely to be related to exposure to workplace violence due to other characteristics, such as job positions or behavior (Aquino and Thau 2009, p. 724; Hindelang et al. 1978).

Work characteristics such as the position in the organization and the feeling of having variability in and control over your job could be factors related to exposure to workplace violence (Aquino and Thau 2009). Overall, employees occupying lower positions in the organization seem to be more often exposed to workplace violence than employees in higher positions. Furthermore, employees who experience low variability in their job seem to be more often exposed to workplace violence than employees experience have more variability. Finally, employees who experience more role conflict and role ambiguity seem to be more often exposed to workplace aggression than employees with less role conflict and ambiguity (Aquino and Thau 2009; Bowling and Beehr 2006). Additionally, the job itself of employees is a factor that seems strongly related to exposure to workplace violence, but these will be described in the paragraph about contexts of workplace violence, as, in general, the job is a strong predictor of the context employees work in.

In addition, psychological characteristics (including behavior) such as affect and dominant or uncivil behavior could be factors related to exposure to workplace violence (Aquino and Thau 2009). Overall, employees who have more propensity to experience negative affect or are more emotional unstable seem to be more often

exposed to workplace violence, compared to employees who have less negative affect and are more emotionally stable. Finally, employees who have more dominant and uncivil behavior seem to be more often exposed to workplace violence. However, in some studies, it was found that also employees with low levels of dominance are more often exposed to workplace violence, that is, that both either relatively high or low levels seem related to more exposure to workplace violence (Aquino and Thau 2009). Victim characteristics, including sociodemographic, work, and psychological characteristics, are thus a group of factors, which seem to contribute to workplace violence, particularly by having either more situational exposure to workplace violence or by being more personally vulnerable to be confronted to workplace violence.

Context Factors

> Firefighters extinguish a fire during New Year's Eve. One of the emergency buildings of a physiotherapist is in flames. During the extinguishing activities, a boy who witnesses the fire shoots fireworks at the fire brigade. (Bergman et al. 2013).

Context factors are an additional group of factors which seem to contribute to workplace violence. First and foremost, the occupational group determines the type of work contexts employees are in and, thus, to what extent workplace violence occurs. Employees working in industry (Aquino and Thau 2009, p. 726) and law enforcement officers (Van Reemst and Fischer 2016) are at relatively high risk of exposure to workplace violence. One of the important related context characteristics is the amount and type of contact between the potential offender and victim. Workplace violence occurs more often in case employees spend more time together, as both co-workers or supervisor-subordinate dyads (Barling et al. 2009). Furthermore, employees who more often have contact with citizens are more often exposed to workplace violence than employees who have less contact with others (LeBlanc and Kelloway 2002). This contact could include physical or verbal contact and could include contact with various citizens, such as those who are more likely to offend (LeBlanc and Kelloway 2002). Therefore, also specific work days during which more contact occurs, such as New Year's Eve, could result in more risk of aggression (see described case).

In addition to the type of contact between people, the broader work context could be related to workplace violence. For example, leaders could fail to provide clear guidelines for what constitutes inappropriate conduct. This could result in workplace violence within the organization (Aquino and Thau 2009, p. 727). In general, a violence prevention climate seems to prevent workplace violence over time (Spector et al. 2015). This violence prevention climate includes management concerns, policies, and practices (and employees' perception on these topics) to cope with workplace violence in the organization (Spector et al. 2015). Context characteristics, including the extent and type of contact between potential offender and victim and policies regarding workplace violence, are thus a group of factors that seem to contribute to workplace violence, especially by having more situational exposure to workplace violence. This group of factors seems to be strongly determined by the occupational group employees work in.

Variations

It is important to note that different factors could be of influence on workplace violence, depending on the occupational group, relationship between offender and victim, and type of aggression. For example, whereas being under the influence of alcohol may contribute to workplace violence enacted by citizens, it is less likely to explain workplace violence enacted by employees, as use of alcohol is less common and accepted during work hours. Another example is that work characteristics seem stronger related to workplace violence among law enforcement officers than firefighters (Van Reemst and Fischer 2016), which was possibly explained by the larger variation within law enforcement officers in work situations and

exposure to workplace violence. Factors thus vary into what extent they contribute to workplace violence. Comparative research is scarce, but this is important to take into account when considering factors that contribute to workplace violence in specific contexts.

Conclusion

This chapter provided a general overview of factors contributing and facilitating workplace violence. Factors that were discussed were related to the (possible) offender, the victim, and the context and may relate to workplace violence through, for example, situational or personal vulnerability processes. In addition, it was highlighted that it may vary to what extent factors contribute to workplace violence. Taking these three groups of factors into account, workplace violence can be seen as an interaction between (possible) offender and (possible) victim in a certain context. As can be seen in the cases that were described at the beginning of each paragraph, often multiple contributing factors can be identified or suggested in a single incident. For example, in the first case of the man urinating in public, also the role of the behavior of the police officers and the context of arresting the man could be suggested to be contributing characteristics. This means that characteristics are likely to interact with each other. For example, an employee who enacted aggression before could particularly enact workplace violence if the other employee (victim) is emotionally unstable and little guidelines are available on workplace violence within the organization. Therefore, workplace violence could especially occur if factors related to higher motivation of offenders, less guardianship (such as guidelines), and more suitableness of the target are all present (cf. Cohen and Felson 1979). Important to note is that research on this topic, which factors contribute to workplace violence, is still ongoing. As has been implied in this chapter, more research is needed on how these characteristics are related to workplace violence over time (do all actually predict workplace violence, or are some a result of workplace violence – or both?), how characteristics interact, and how they vary between occupational groups, relationships between offender and victim, and types of aggression. In addition, more information is needed about to what extent this knowledge translates to effective interventions to reduce, prevent, or cope with workplace aggression.

Cross-References

- ▶ Workplace Violence: Assault
- ▶ Workplace Violence: Past and Current Employees

References

Aquino, K., & Thau, S. (2009). Workplace victimization: Aggression from the target's perspective. *Annual Review of Psychology, 60*, 717–741. https://doi.org/10.1146/annurev.psych.60.110707.163703.

Barling, J., Dupré, K. E., & Kelloway, E. K. (2009). Predicting workplace aggression and violence. *Annual Review of Psychology, 60*, 671–692. https://doi.org/10.1146/annurev.psych.60.110707.163629.

Bergman, E., Valk, H., & de Vries, M. (2013). *Agressie tegen publieke dienstverleners*. Apeldoorn: Maklu.

Bowling, N. A., & Beehr, T. A. (2006). Workplace harassment from the victim's perspective: A theoretical model and meta-analysis. *Journal of Applied Psychology, 91*(5), 998–1012. https://doi.org/10.1037/0021-9010.91.5.998.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger Publishing Company.

LeBlanc, M., & Kelloway, E. (2002). Predictors and outcomes of workplace violence and aggression. *Journal of Applied Psychology, 87*(3), 444–453. https://doi.org/10.1037//0021-9010.87.3.444.

Penney, L., Martir, A., & Bok, C. (2017). Environmental antecedents of workplace aggression: A review and examination of psychological process. In N. Bowling & M. Hershcovis (Eds.), *Research and theory on workplace aggression* (pp. 34–61). New York: Cambridge University Press.

Schat, A. C., & Frone, M. R. (2011). Exposure to psychological aggression at work and job performance: The mediating role of job attitudes and personal health.

Work & Stress, 25(1), 23–40. https://doi.org/10.1080/02678373.2011.563133.
Spector, P. E., Yang, L., & Zhou, Z. E. (2015). A longitudinal investigation of the role of violence prevention climate in exposure to workplace physical violence and verbal abuse. *Work & Stress, 29*(4), 325–340. https://doi.org/10.1080/02678373.2015. 1076537.
Van Reemst, L., & Fischer, T. F. C. (2016). Experiencing external workplace violence: Differences in indicators between three types of emergency responders. *Journal of Interpersonal Violence*. https://doi.org/10.1177/0886260516657913.
Wolfgang, M. E. (1958). *Patterns in criminal homicide*. Oxford: University of Pennsylvania Press.

Further Reading

Bowling, N. A., & Hershcovis, M. S. (2017). *Research and theory on workplace aggression* (Current perspectives in social and behavioral sciences). New York: Cambridge University Press.
Van Reemst, L. (forthcoming). *Emergency responders at risk: An empirical analysis of the relationship between emergency responders' characteristics and their exposure to aggression from citizens*. Unpublished doctoral dissertation, Erasmus University Rotterdam, The Netherlands.

Workplace Violence: Intimate Partner Violence

E. Kevin Kelloway
Department of Psychology, Saint Mary's University, Halifax, NS, Canada

Keywords
Active shooter · Domestic violence · Employee health risks · Stalking · Intimate partner harassment · Partner violence and work

Definition

As defined by the Centers for Disease Control and Prevention in the United States, intimate partner violence comprises threatened or actual violence or aggression (including sexual violence) directed at a current or former spouse or partner (c.f., Swanberg et al. 2006). Although this definition includes non-violent acts of aggression, more recently researchers have also used the term intimate partner aggression (LeBlanc et al. 2014) to refer to non-violent abuse within a current or former relationship.

Introduction

Intimate partner violence (IPV) can include same sex as well as heterosexual relationships. More commonly, intimate partner violence may also be referred to as domestic violence or as family violence. Although intimate partner violence originates outside of the workplace, it may spillover into the workplace or have consequences for employees' workplace behavior. As a result, intimate partner violence is a concern for workplace safety. This chapter reviews the incidence of IPV, consequences for both the individual and the organization, and possible interventions.

Prevalence of Intimate Partner Violence

Globally almost 30% of women report experiencing intimate partner violence at some point in their life (WHO 2013), with men experiencing intimate partner violence at a lower rate. In the United States, more than one in three women and one in four men are exposed to intimate partner violence at some point in their lives (Black et al. 2011). Intimate partners are identified as the perpetrator in approximately 1–3% of all workplace violence incidents (Duhart 2001).

As Swanberg et al. (2006) noted, prevalence rates may be underestimates as victims may not disclose or report on surveys. Moreover, official statistics may not record whether or not the perpetrator was a current or former partner. Despite these concerns, it is clear that intimate partner violence is a serious social problem in many parts of the world (WHO 2013) with substantial consequences for both individuals and organizations.

Individual Consequences of Intimate Partner Violence

There is a substantial body of literature that speaks to the significant mental and physical health

consequences of being a victim of intimate partner violence (Wathen et al. 2018). Of course, to the extent that the relationship involves physical violence, the risk of physical injury is clear and easy to understand. However, research has also identified a host of mental health disorders resulting from exposure to intimate partner violence. These include post-traumatic stress disorder (PTSD), eating disorders, sleep disorders, depression, and anxiety in addition to substance use disorders (Wathen et al. 2018). Victims of intimate partner violence may also experience a range of physical effects including chronic pain and cardiac disease as well as engaging in suicide attempts or self-harm.

As Wathen et al. (2018) note, there is an economic cost to intimate partner violence that accrues to both the victim and to society. Individuals may experience wage loss as a result of their inability to continue working while being victimized (see below), and these effects may be magnified through career interruptions and disrupted career progression for the individual exposed to intimate partner violence. Tolentino et al. (2017) found that women exposed to intimate partner violence were rated as engaging in lower levels of in-role (i.e., task) and extra-role (i.e., organizational citizenship) behaviors and, as a result, were seen as being less promotable by their supervisors than those actively engaged.

Organizational Consequences of Intimate Partner Violence

There are at least four ways in which intimate partner violence may affect, or manifest in, the workplace. First, consistent with the array of health effects previously discussed, victims of intimate partner violence may display impaired work performance or interpersonal interactions. Dimoff and Kelloway (in press), for example, found that individuals experiencing a crisis such as a mental health problem would display behavioral signs such as withdrawing from others in the workplace (e.g., not going for coffee or lunch, restricting interactions), expressions of emotional distress (e.g., crying or stating that they were stressed), engaging in extreme behaviors (e.g., theft, threats of self-harm, lack of personal hygiene), absenteeism or tardiness, and impaired quantity or quality of job performance. Consistent with this view, LeBlanc et al. (2014) reported that victims of intimate partner aggression demonstrated withdrawal at work (e.g., cognitive distraction, neglect of work), withdrawal from work (e.g., absenteeism, tardiness), and impaired job performance. Even when the intimate partner violence does not occur at the workplace, the signs of victimization may be evident in the workplace and significantly affect organizational outcomes such as attendance and job performance.

Second, intimate partner violence can occur at the workplace. For many individuals, work is a "social address." That is, partners or family members know where the person works and, often, his or her schedule. An individual intent on harming a partner may show up at that partner's workplace where they know he/she will be. Even when physical violence is not the intent, a confrontation, and attendant embarrassment of the partner, may be a form of intimate partner violence.

Third, and relatedly, a perpetrator may "stalk" his or her partner. Repeated phone calls, texts, and emails may be sent to disrupt the victim's workday. The perpetrator may wait outside the workplace for the victim to go to lunch or leave the workplace in order to provoke a confrontation. Simply being seen hanging around the workplace may be sufficient to provoke a feeling of being unsafe in the victim. Although this form of intimate partner violence does not involve the perpetrator entering the workplace, the clear intent of such actions is to disrupt the work performance of the victim.

Finally, the perpetrator can take action to interfere with the victim's ability to do, or get to, work. Disabling their car, hiding car keys, hiding clothes, or denying access to a home computer may all be ways of interfering with the victim's ability to work – again, without the perpetrator actually entering the workplace. Refusing to provide childcare may also interfere with the victim's ability to attend work as scheduled (Swanberg et al. 2006).

Interventions for Intimate Partner Violence

Intimate partner violence can, but usually does not, happen at the workplace and, as a result, may be seen as a "private" issue with which organizations should not be concerned. As the preceding review attests, nothing could be further from the truth – although intimate partner violence may not occur in the workplace, its effects manifest in the workplace and directly affect organizational functioning. Organizations have both a moral and a pragmatic rationale for taking action to assist individuals who are exposed to intimate partner violence. Organizational responses can include primary (i.e., providing specific security measures to assist employees), secondary (i.e., providing a supportive environment to help employees) and tertiary (i.e., providing access to mental health and other resources) interventions.

First, organizations can take specific actions to deal with the threat of intimate partner violence in the workplace and enhance the security of employees while at the workplace. Ensuring secure access to the worksite, escorting individuals to and from the parking lot before and after work, and screening calls are all actions that organizations can take to assist victims of intimate partner violence (Swanberg et al. 2007). Although these often emerge as responses to specific threats, a comprehensive workplace violence prevention plan should recognize the possibility, and take steps to mitigate the risk, of workplace violence resulting from intimate partner violence (Kelloway et al. 2017).

Second, a supportive environment may mitigate some of the negative workplace consequences of intimate partner violence. Tolentino et al. (2017), for example, found that organizational support moderated the effects of reduced job performance and organizational citizenship on supervisors' assessment of promotability. Organizations that make the effort to educate managers about intimate partner violence can create a culture in which being a victim is destigmatized, and the emphasis is placed on helping individuals in crisis rather than disciplining individuals for absenteeism, tardiness, or reduced job performance (for an analogous approach to mental health disorders, see Dimoff et al. 2016). Swanberg et al. (2007) found that listening with an open ear, sitting with a victim during a break, and providing individuals with increased flexibility (e.g., around schedules or workload) were all means of organizational support for individuals exposed to intimate partner violence.

Finally, organizations can also provide individuals exposed to intimate partner violence with access to resources to deal with specific issues. For example, Swanberg et al. (2007) found that organizations offered employees a referral through a counsellor or Employee Assistance Program for assistance with dealing with the strain of intimate partner violence. Although there is a lack of data supporting the effectiveness of Employee Assistance Programs for intimate partner violence, there is evidence suggesting that short-term psychotherapeutic interventions – particularly those based on cognitive behavioral therapy – can be of significant benefit to victims of intimate partner violence (Arroyo et al. 2017). Swanberg et al. (2007) reported that organizations could also provide information in the form of brochures or referrals to community-based organizations as a form of support to victims of intimate partner violence. Organizations that build links to these community resources are in a better position to both educate themselves about and offer support for individuals dealing with intimate partner violence.

Conclusion

Intimate partner violence – violence and aggression that occurs within a current or previous relationship – is a prevalent social phenomenon affecting more than a third of women and more than 25% of men in the United States. Individuals exposed to intimate partner violence can experience a wide range of physical and psychological disorders, many of which can last long after the exposure to violence has ended. Although not typically recognized as a workplace problem, it is clear that intimate partner violence (a) can manifest in the workplace by adversely affecting the ability of the victim to attend or focus on work and

(b) can occur in the workplace as perpetrators use the workplace as a social address for victims. Organizations have a role to play in addressing intimate partner violence by providing a supportive climate in the organization, by providing individuals with specific resources to deal with intimate partner violence, and by providing enhanced safety provisions for victims as part of a comprehensive workplace violence prevention program. Human resource policies that encourage individuals to report experiencing intimate partner violence allow organizations to provide supports to individuals as well as take steps to protect all individuals in the workplace.

Cross-References

- ▶ Workplace Violence: Active Shooter/Terrorist Threats
- ▶ Workplace Violence: Factors Contributing and/or Facilitating
- ▶ Workplace Violence: Intimate Partner Violence

References

Arroyo, K., Lundahl, B., Butters, R., Vanderloo, M., & Wood, D. S. (2017). Short-term interventions for survivors of intimate partner violence: A systematic review and meta-analysis. *Trauma, Violence & Abuse, 18*(2), 155–171.

Black, M. C., Basile, K. C., Breiding, M. J., Smith, S. G., Walters, M. L., Merrick, M. T., et al. (2011). *The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 summary report*. Atlanta: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.

Dimoff, J. K., & Kelloway, E. K. (in press). Signs of struggle (SOS): The development and validation of a behavioural mental health checklist for the workplace. *Work & Stress*. https://doi.org/10.1080/02678373.2018.1503359.

Dimoff, J. K., Kelloway, E. K., & Burnstein, M. D. (2016). Mental health awareness training (MHAT): The development and evaluation of an intervention for workplace leaders. *International Journal of Stress Management, 23*(2), 167.

Duhart, D. T. (2001). *Special report: Violence in the workplace, 1993–99*. Washington, DC: U.S. Department of Justice.

Kelloway, E. K., Francis, L. D., & Gatien, B. (2017). *Management of occupational health and safety*. Toronto: Nelson.

LeBlanc, M. M., Barling, J., & Turner, N. (2014). Intimate partner aggression and women's work outcomes. *Journal of Occupational Health Psychology, 19*(4), 399.

Swanberg, J., Logan, T., & Macke, C. (2006). The consequences of partner violence on employment and the workplace. In E. Kevin Kelloway, J. Barling, & J. Hurrell Jr. (Eds.), *Handbook of workplace violence* (pp. 351–380). Thousand Oaks: Sage.

Swanberg, J., Macke, C., & Logan, T. K. (2007). Working women making it work: Intimate partner violence, employment, and workplace support. *Journal of Interpersonal Violence, 22*(3), 292–311.

Tolentino, L. R., Garcia, P. R. J. M., Restubog, S. L. D., Scott, K. L., & Aquino, K. (2017). Does domestic intimate partner aggression affect career outcomes? The role of perceived organizational support. *Human Resource Management, 56*(4), 593–611.

Wathen, C. N., MacGregor, J. C., & MacQuarrie, B. J. (2018). Relationships among intimate partner violence, work, and health. *Journal of Interpersonal Violence, 33*(14), 2268–2290.

World Health Organization. (2013). Global and regional estimates of violence against women: Prevalence and health effects of intimate partner violence and non-partner sexual violence. In *Global and regional estimates of violence against women Prevalence and health effects of intimate partner violence and non-partner sexual violence*. Geneva: World Health Organization.

Further Reading

LeBlanc, M. M., Barling, J., & Turner, N. (2014). Intimate partner aggression and women's work outcomes. *Journal of Occupational Health Psychology, 19*(4), 399.

Swanberg, J., Logan, T., & Macke, C. (2006). The consequences of partner violence on employment and the workplace. In E. Kevin Kelloway, J. Barling, & J. Hurrell Jr. (Eds.), *Handbook of workplace violence* (pp. 351–380). Thousand Oaks: Sage.

Workplace Violence: Past and Current Employees

Tabatha Thibault[1] and E. Kevin Kelloway[2]
[1]Saint Mary's University, Halifax, NS, Canada
[2]Department of Psychology, Saint Mary's University, Halifax, NS, Canada

Keywords

Workplace violence · Workplace aggression · Counterproductive work behavior · Personality · Justice

Definition

Workplace violence can be defined as any employee behavior designed to harm (either physically or psychologically) an individual in the workplace (Day and Catano 2006; Dillon 2012).

Introduction

Roughly 50% of large American organizations (those with at least one thousand employees) reported an incident of workplace violence (United States Department of Labor, Bureau of Labor Statistics, and Survey of Workplace Violence Prevention 2005). In Canada, 21% of employees sampled reported experience some form of workplace violence, while 14% said that they experienced workplace violence within the last 2 years (Employment and Social Development Canada 2017). Workplace violence can encompass various types of deviant behaviors that produce harm physically or psychologically (Demir and Rodwell 2012), such as bullying (i.e., persistent acts of aggression toward an individual; Nielsen and Einarsen 2012), incivility (i.e., rude or discourteous behaviors with ambiguous intent; Leiter et al. 2011), and sexual harassment (unwelcomed sexual conduct or comment; Lee 2018). Aggression and violence are often used synonymously in the literature (Day and Catano 2006). This entry will treat these terms as synonyms but will maintain the original term(s) used in each source referenced.

Workplace violence (in any form) has a negative impact on both employees and the organization (Hogh and Viitasara 2005; Nielsen and Einarsen 2012). For example, coworker aggression has been negatively linked to emotional well-being and psychosomatic well-being as well as affective organizational commitment (LeBlanc and Kelloway 2002). In their systematic review, Hogh and Viitasara (2005) found several cognitive (e.g., trying to understand the event after the fact), emotional (e.g., anger, poor mental health, distress, fatigue, anxiety), and psychosomatic symptoms (e.g., tension) resulting from nonfatal workplace violence. Based on meta-analytic evidence, experiencing workplace bullying is associated with anxiety, depression, somatization, physical health problems, post-traumatic stress, burnout, and strain (Nielsen and Einarsen 2012). Bullying and sexual harassment are also positively related to psychological distress (Demir and Rodwell 2012). Organizational outcomes related to workplace bullying include increased intent to leave and absenteeism and decreased organizational commitment and job satisfaction (Demir and Rodwell 2012; Nielsen and Einarsen 2012).

Various antecedents of employee violence have been examined over the years; these include biological factors (e.g., gender), individual differences (i.e., personality traits), environmental or work-related factors (e.g., organizational justice, organizational culture), reactions to events (e.g., being a victim of bullying), and social issues (e.g., social norms; Day and Catano 2006; Trépanier et al. 2015). There is a fairly common (but unsupported) perception that layoffs can lead to aggression. Unemployment and layoffs can indeed cause anger and frustration that could lead to aggression (Catalano et al. 1997, 2002), but it is these emotions that influence violent behaviors, not the layoffs themselves (Barling et al. 2009). The majority of former employees do not take their anger out on the organization, despite potential feelings of bitterness (Fox and Levin 1994).

This chapter will briefly summarize the research on antecedents of workplace violence – both individual differences and environmental factors – committed by past and current employees (i.e., organizational insiders). However, it is important to note that the majority of workplace violence incidents (e.g., 90% of nonfatal workplace assaults; Peek-Asa and Howard 1999; 85% of workplace homicides; Sygnatur and Toscano 2000) are committed by organizational outsiders (e.g., customers, acquaintances, or those engaging in robberies or other crimes; Barling et al. 2009; McPhaul and Lipscomb 2004; Peek-Asa and Howard 1999) and are beyond the scope of this paper.

Individual Differences

The Big Five personality traits have been tied to aggressive work behaviors (Day and Catano 2006; Ones and Viswesvaran 2001). A meta-analysis by Grijalva and Newman (2015) found that agreeableness (i.e., kind, considerate, trusting) and conscientiousness (i.e., organized, responsible, thoughtful) were negatively correlated with measures of counterproductive work behaviors (CWB), while neuroticism (i.e., anxious, insecure) had a positive association with CWB. Agreeableness is most strongly associated with CWBs directed at individuals (CWB-I; e.g., Berry et al. 2007). Additionally, agreeableness has been shown to predict organizational retaliatory behavior (i.e., behaviors such as sabotage or assault due to perceived unfairness; Skarlicki et al. 1999). Spector and Zhou (2014) found that relational aggression was negatively related to agreeableness, conscientiousness, and emotional stability (the reverse of neuroticism). Agreeableness and honesty-humility (said to be the sixth personality trait; i.e., sincere and fair, lacking in greed and conceit; Lee and Ashton 2004) have been found to negatively predict antisocial behavior directed toward individuals (ASB-I), while extraversion seems to positively predict ASB-I (Lee et al. 2005). ASB is similar to counterproductive work behavior (CWB), when directed at individuals; there is some intent to harm those individuals.

Negative emotions and personality traits related to negative emotions have been linked to workplace aggression. Anger and frustration can lead an employee to engage in workplace violence (Fox and Spector 1999). Trait anger (i.e., a predisposition to anger and respond with hostility) is positively related to aggression directed toward both individuals and the organization (Hershcovis et al. 2007). The type A behavioral pattern (i.e., a set of characteristics including a proneness to irritability, impatience, competitiveness, and hostility) is also linked to workplace aggression (Baron et al. 1999). Somewhat similarly, Douglas and Martinko (2001) found that a hostile attribution style is positively corrected with both general workplace aggression and relational aggression.

Researchers have also looked at specific personality traits as predictors of workplace aggression. Negative affectivity (i.e., a tendency to experience general distress and aversive mood states such as anger and nervousness; Douglas and Martinko 2001) has been positively linked to interpersonal and organizational aggression (Hershcovis et al. 2007), overall workplace aggression (Douglas and Martinko 2001), and organizational retaliatory behavior (Skarlicki et al. 1999). Workplace aggression is negatively correlated with self-control, indicating that a lack of self-control can foster aggression (Douglas and Martinko 2001). Somewhat similarly, an external locus of control (i.e., a belief that one's source of control is due to external forces) is associated with overall behavioral reactions to frustrating conditions, specifically sabotage (Storms and Spector 1987).

Several other factors more internal to a person have been examined as possible antecedents. For instance, attitudes toward revenge are correlated with workplace aggression (Douglas and Martinko 2001). There is some mixed evidence that alcohol use may be linked to workplace violence (specifically directed at coworkers); however this tends to only hold under certain environmental factors (e.g., job insecurity or perceived injustice; Greenberg and Barling 1999). Past behavior is usually a good indication of future behavior; this statement holds for workplace violence (Day and Catano 2006). A history of aggression has been linked to engaging in workplace aggression as an adult (Greenberg and Barling 1999; Inness et al. 2005). In the next section, the role of environmental factors on employees' proneness to violence is explored.

Environmental Factors

Despite all the research on the personality determinants of workplace violence, meta-analytic

data show that workplace or environmental factors are more strongly correlated and explain significantly more variance in workplace aggression than do individual differences (Hershcovis et al. 2007; Inness et al. 2005). For instance, Inness, Barling, and Turner (2005) found that abusive supervision predicted workplace aggression above and beyond demographic variables, self-esteem, and history of aggression. Individual differences can actually moderate the relationship between situational factors and violent behaviors (Harris et al. 2010; Taylor and Kluemper 2012). For example, Colbert, Mount, Harter, Witt, and Barrick (2004) found that agreeableness moderated the relationship between perceived organizational support and interpersonal deviance such that the relationship was negative when agreeableness was low but positive when agreeableness was high.

There is a great deal of evidence on the link between perceived injustice and workplace violence (e.g., Baron et al. 1999; Inness et al. 2005). There are three general types of justice: procedural (i.e., perceived fairness of organizational decisions and procedures), distributive (i.e., perceived fairness of distributive outcomes), and interactional (i.e., perceived fairness of interpersonal treatment; Greenberg and Barling 1999). Using a meta-analysis, Hershcovis et al. (2007) found a correlation between distributive and procedural justice and interpersonal-targeted aggression and organizational aggression. Interpersonal justice, a type of interactional justice, is also related to workplace aggression (Dupré et al. 2006). Similarly, procedural justice has been found to negatively predict aggression toward a supervisor (Greenberg and Barling 1999). That said, individual differences (specifically negative affect and agreeableness) appear to moderate the relationship between perceived injustice and retaliatory behavior (Skarlicki et al. 1999).

Researchers have examined many organizational variables in relation to enacted aggression; these include job-related factors (e.g., workload; Baillien et al. 2011), supervisory-related factors (e.g., abusive supervision; Inness et al. 2005), interpersonal factor (e.g., conflict; Hauge et al. 2009), and job attitudes (e.g., job satisfaction; Hershcovis et al. 2007). Bentley, Cathley, Forsyth, and Tappin (2014) noted three workplace violence risk factors, namely, time pressure, workload, and communication. Greenberg and Barling (1999) found that workplace surveillance was positively related to aggression against one's supervisor. Interpersonal conflict, job dissatisfaction, and situational constraints have also been tied to interpersonal-targeted aggression and organizational aggression (Hershcovis et al. 2007). Other workplace variables linked to workplace aggression include (but are not limited to) role conflict, role overload, role ambiguity, work constraints, job autonomy, and perceived violence climate (Barling et al. 2009).

Organizational variables or environmental factors have also been tied to specific forms of workplace violence. For instance, instigated incivility (i.e., engaging in incivility) has been positively associated with organizational change, job insecurity, job demands, and experiencing incivility (from coworkers) and negatively associated with social support (from coworkers; Torkelson et al. 2016). Having a supervisor who engages in passive leadership (i.e., a lack of leadership behaviors) is linked to observed hostility (displayed by organizational members) and employees experiencing sexual harassment (Lee 2018).

Workload, job stress, lack of job autonomy, and uncivil climate are correlated with engaging in workplace bullying (Baillien et al. 2011; Goodboy et al. 2017; Taylor and Kluemper 2012). Job demands and resources have also been linked to bullying (Balducci et al. 2011). Specifically, workload and role conflict are positively associated with bullying, while decision authority, coworker support, and salary/promotion prospects are negatively associated with bullying (Balducci et al. 2011). Leader-member exchange (LMX; i.e., the quality and type of dyadic relationship exchanges between a subordinate and a supervisor; Ilies et al. 2007) has also been shown to negatively predict bullying (Porter et al. 2018). Based on meta-analytic data,

workplace harassment (i.e., interpersonal behavior meant to harm a target at work; simply another term for workplace bullying) is positively associated with role conflict, role ambiguity, role overload, and work constraints and negatively related to autonomy (Bowling and Beehr 2006).

Conclusion and Recommendations

Workplace violence has a negative impact on organizations and their employees. Various individual differences (such as personality traits) and situational factors (e.g., organizational injustice) are related to and can cause an employee to engage in aggressive behaviors at work. Often these individual differences and environmental factors interact. Despite the tendency to blame an (current or former) employee's predisposition to aggression, it is up to the organization to create and maintain an environment that will reduce the likelihood of its employees acting in this deviant manner. The use of multiple methods is more advisable than using a single preventative measure (Ta and Loomis 2007). Organizations should create policies and practices that outline acceptable behavior as well as working to instill an organizational culture with positive values (Bentley et al. 2014). Ta and Loomis (2007) advised considering hazards within the workforce, as well as community and industry characteristics, when designing or planning intervention efforts.

As a broad statement, organizations can make efforts to reduce job demands and increase job resources to decrease behaviors, such as bullying and interpersonal conflicts (Balducci et al. 2011). For instance, providing employees with role clarification could reduce a job demand (i.e., ambiguity; Bowling and Beehr 2006). Simply increasing communication among employees and throughout the organizational hierarchy may even reduce behaviors such as bullying (Bentley et al. 2014). Decreasing employee stress through reducing or removing workplace stressors can help lessen workplace harassment and bullying (Bowling and Beehr 2006). On a similar note, educating employees on ways to cope with stress and changing the way they appraise or react to stressors would also be beneficial.

Various types of training interventions can be used to help prevent workplace violence. For instance, bullying may be reduced by providing employees with conflict management training (Balducci et al. 2011). Leadership training (e.g., transformational or ethical leadership training) would be an effective intervention that can not only reduce workplace violence (Lee 2018) but have several other benefits (e.g., increase employee well-being and safety; McKee et al. 2018; von Thiele Schwarz et al. 2016). As passive leadership is associated with hostility and sexual harassment, leaders should be encouraged to take on an active role in their workplace and ensure they do not appear apathetic to harassing or aggressive behaviors (Lee 2018). Bystander interventions or awareness training for either managers or employees may also combat workplace violence, especially those behaviors that may be more ambiguous (Lee 2018; McDonald et al. 2016). For instance, sexual harassment training can increase participants' sensitivity to the type of behavior in question (Buckner et al. 2014).

When looking at minimizing the possibility of vengeful ex-employees, the approach is similar to reducing workplace violence perpetrated by current employees. Ensure that proper systems and procedures are in place, such as grievance, appeal, and harassment procedures (Fox and Levin 1994). Consider offering new former employees job-retraining options or opportunities (especially if these employees held a long tenure at the organization). In short, continue to treat these people with respect. Escorting newly fired employees from the building with security personnel will be less effective than simply showing that the organization still cares and respects their former employees (Fox and Levin 1994). That said, there are times when the risk of violence might be high (e.g., during labor disputes, disgruntled former employees following layoff or dismissal; Francis et al. 2006). In these circumstances heightened security precautions (e.g., restricting access to the workplace) might be prudent.

Cross-References

- ▶ Personnel Security: Selection
- ▶ Workplace Violence: Assault
- ▶ Workplace Violence: Factors Contributing and/or Facilitating
- ▶ Workplace: Hostile Environment
- ▶ Workplace: Sexual Harassment

References

Baillien, E., De Cuyper, N., & De Witte, H. (2011). Job autonomy and workload as antecedents of workplace bullying: A two-wave test of Karasek's Job Demand Control Model for targets and perpetrators. *Journal of Occupational and Organizational Psychology, 84*(1), 191–208. https://doi.org/10.1348/096317910X508371.

Balducci, C., Fraccaroli, F., & Schaufeli, W. B. (2011). Workplace bullying and its relation with work characteristics, personality, and post-traumatic stress symptoms: An integrated model. *Anxiety, Stress, and Coping, 24*(5), 499–513. https://doi.org/10.1080/10615806.2011.555533.

Barling, J., Dupré, K. E., & Kelloway, E. K. (2009). Predicting workplace aggression and violence. *Annual Review of Psychology, 60*, 671–692. https://doi.org/10.1146/annurev.psych.60.110707.163629.

Baron, R. A., Neuman, J. H., & Geddes, D. (1999). Social and personal determinants of workplace aggression: Evidence for the impact of perceived injustice and the Type A behavior pattern. *Aggressive Behavior, 25*(4), 281–296.

Bentley, T. A., Catley, B., Forsyth, D., & Tappin, D. (2014). Understanding workplace violence: The value of a systems perspective. *Applied Ergonomics, 45*, 839–848. https://doi.org/10.1016/j.apergo.2013.10.016.

Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology, 92*, 410–424. https://doi.org/10.1037/0021-9010.92.2.410.

Bowling, N. A., & Beehr, T. A. (2006). Workplace harassment from the victim's perspective: A theoretical model and meta-analysis. *Journal of Applied Psychology, 91*(5), 998–1012. https://doi.org/10.1037/0021-9010.91.5.998.

Buckner, G. E., Hindman, H. D., Huelsman, T. J., & Bergman, J. Z. (2014). Managing workplace sexual harassment: The role of manager training. *Employee Responsibilities and Rights Journal, 26*(4), 257–278.

Catalano, R., Novaco, R., & McConnell, W. (1997). A model of the net effect of job loss on violence. *Journal of Personality and Social Psychology, 72*(6), 1440–1447.

Catalano, R., Novaco, R. W., & McConnell, W. (2002). Layoffs and violence revisited. *Aggressive Behavior, 28*, 233–247. https://doi.org/10.1002/ab.80003.

Colbert, A. E., Mount, M. K., Harter, J. K., Witt, L. A., & Barrick, M. R. (2004). Interactive effects of personality and perceptions of the work situation on workplace deviance. *Journal of Applied Psychology, 89*(4), 599–609. https://doi.org/10.1037/0021-9010.89.4.599.

Day, A. L., & Catano, V. M. (2006). Screening and selecting out violent employees. In E. K. Kelloway, J. Barling, & J. J. Hurrell (Eds.), *Handbook of workplace violence* (pp. 549–577). Thousand Oaks: Sage.

Demir, D., & Rodwell, J. (2012). Psychosocial antecedents and consequences of workplace aggression for hospital nurses. *Journal of Nursing Scholarship, 44*(4), 376–384. https://doi.org/10.1111/j.1547-5069.2012.01472.x.

Dillon, B. L. (2012). Workplace violence: Impact, causes, and prevention. *Work, 42*(1), 15–20. https://doi.org/10.3233/WOR-2012-1322.

Douglas, S. C., & Martinko, M. J. (2001). Exploring the role of individual differences in the prediction of workplace aggression. *Journal of Applied Psychology, 86*, 547–559. https://doi.org/10.1037/0021-9010.86.4.547.

Dupré, K. E., Inness, M., Connelly, C. E., Barling, J., & Hoption, C. (2006). Workplace aggression in teenage part-time employees. *Journal of Applied Psychology, 91*(5), 987–997. https://doi.org/10.1037/0021-9010.91.5.987.

Employment and Social Development Canada. (2017). *Harassment and sexual violence in the workplace public consultations – What we heard*. Retrieved from https://www.canada.ca/en/employment-social-development/services/health-safety/reports/workplace-harassment-sexual-violence.html#h2.2-h3.2

Fox, J. A., & Levin, J. (1994). Firing back: The growing threat of workplace homicide. *The Annals of the American Academy of Political and Social Science, 536*(1), 16–30.

Fox, S., & Spector, P. E. (1999). A model of work frustration-aggression. *Journal of Organizational Behavior, 20*(6), 915–931.

Francis, L., Cameron, J. E., & Kelloway, E. K. (2006). Crossing the line: Violence on the picket line. In *Handbook of workplace violence* (pp. 231–260). Thousand Oaks: Sage. https://doi.org/10.4135/9781412976947.n11.

Goodboy, A. K., Martin, M. M., Knight, J. M., & Long, Z. (2017). Creating the boiler room environment: The job demand-control-support model as an explanation for workplace bullying. *Communication Research, 44*(2), 244–262.

Greenberg, L., & Barling, J. (1999). Predicting employee aggression against coworkers, subordinates and supervisors: The roles of person behaviors and perceived workplace factors. *Journal of Organizational Behavior, 20*(6), 897–913.

Grijalva, E., & Newman, D. A. (2015). Narcissism and counterproductive work behavior (CWB): Meta-

analysis and consideration of collectivist culture, Big Five personality, and narcissism's facet structure. *Applied Psychology. An International Review, 64*, 93–126. https://doi.org/10.1111/apps.12025.

Harris, K. J., Harvey, P., & Booth, S. L. (2010). Who abuses their coworkers? An examination of personality and situational variables. *The Journal of Social Psychology, 150*(6), 608–627. https://doi.org/10.1080/00224540903365489.

Hauge, L. J., Skogstad, A., & Einarsen, S. (2009). Individual and situational predictors of workplace bullying: Why do perpetrators engage in the bullying of others? *Work and Stress, 23*(4), 349–358. https://doi.org/10.1080/02678370903395568.

Hershcovis, M. S., Turner, N., Barling, J., Arnold, K. A., Dupré, K. E., Inness, M., ... Sivanathan, N. (2007). Predicting workplace aggression: A meta-analysis. *Journal of Applied Psychology, 92*, 228–238. https://doi.org/10.1037/0021-9010.92.1.228.

Hogh, A., & Viitasara, E. (2005). A systematic review of longitudinal studies of nonfatal workplace violence. *European Journal of Work and Organizational Psychology, 14*, 291–313. https://doi.org/10.1080/13594320500162059.

Ilies, R., Nahrgang, J. D., & Morgeson, F. P. (2007). Leader-member exchange and citizenship behaviors: A meta-analysis. *Journal of Applied Psychology, 92*, 269–277. https://doi.org/10.1037/0021-9010.92.1.269.

Inness, M., Barling, J., & Turner, N. (2005). Understanding supervisor-targeted aggression: A within-person, between-jobs design. *Journal of Applied Psychology, 90*(4), 731–739. https://doi.org/10.1037/0021-9010.90.4.731.

LeBlanc, M. M., & Kelloway, E. K. (2002). Predictors and outcomes of workplace violence and aggression. *Journal of Applied Psychology, 87*, 444–453. https://doi.org/10.1037//0021-9010.87.3.444.

Lee, J. (2018). Passive leadership and sexual harassment: Roles of observed hostility and workplace gender ratio. *Personnel Review, 47*(3), 594–612. https://doi.org/10.1108/PR-07-2016-0169.

Lee, K., & Ashton, M. C. (2004). Psychometric properties of the HEXACO personality inventory. *Multivariate Behavioral Research, 39*(2), 329–358.

Lee, K., Ashton, M. C., & Shin, K. (2005). Personality correlates of workplace anti-social behavior. *Applied Psychology. An International Review, 54*, 81–98. https://doi.org/10.1111/j.1464-0597.2005.00197.x.

Leiter, M. P., Spence Laschinger, H. K., Day, A., & Gilin Oore, D. (2011). The impact of civility interventions on employee social behavior, distress and attitudes. *Journal of Applied Psychology, 96*, 1258–1274. https://doi.org/10.1037/a0024442.

McDonald, P., Charlesworth, S., & Graham, T. (2016). Action or inaction: Bystander intervention in workplace sexual harassment. *The International Journal of Human Resource Management, 27*(5), 548–566. https://doi.org/10.1080/09585192.2015.1023331.

McKee, M., Driscoll, C., Kelloway, E. K., & Kelley, E. (2018). Lifting leaders and their employees to higher levels of well-being: Results from a transformational leadership field development program. Unpublished manuscript.

McPhaul, K. M., & Lipscomb, J. A. (2004). Workplace violence in health care: Recognized but not regulated. *Online Journal of Issues in Nursing, 9*(3), 7.

Nielsen, M. B., & Einarsen, S. (2012). Outcomes of exposure to workplace bullying: A meta-analytic review. *Work and Stress, 26*, 309–332. https://doi.org/10.1080/02678373.2012.734709.

Ones, D. S., & Viswesvaran, C. (2001). Integrity tests and other criterion-focused occupational personality scales (COPS) used in personnel selection. *International Journal of Selection and Assessment, 9*(1/2), 31–39.

Peek-Asa, C., & Howard, J. (1999). Workplace-violence investigations by the California division of occupational safety and health, 1993–1996. *Journal of Occupational and Environmental Medicine, 41*(8), 647–653.

Porter, T. H., Day, N., & Meglich, P. (2018). City of discontent? The influence of perceived organizational culture, LMX, and newcomer status on reported bullying in a municipal workplace. *Employee Responsibilities and Rights Journal, 30*(2), 119–141. https://doi.org/10.1007/s10672-017-9310-8.

Skarlicki, D. P., Folger, R., & Tesluk, P. (1999). Personality as a moderator in the relationship between fairness and retaliation. *Academy of Management Journal, 42*(1), 100–108. https://doi.org/10.2307/256877.

Spector, P. E., & Zhou, Z. E. (2014). The moderating role of gender in relationships of stressors and personality with counterproductive work behavior. *Journal of Business and Psychology, 29*(4), 669–681. https://doi.org/10.1007/s10869-013-9307-8.

Storms, P. L., & Spector, P. E. (1987). Relationships of organizational frustration with reported behavioural reactions: The moderating effect of locus of control. *Journal of Occupational Psychology, 60*(3), 227–234. https://doi.org/10.1111/j.2044-8325.1987.tb00255.x.

Sygnatur, E. F., & Toscano, G. A. (2000). Work-related homicides: The facts. *Compensation and Working Conditions, 5*(1), 3–8.

Ta, M. L., & Loomis, D. P. (2007). Frequency and determinants of recommended workplace violence prevention measures. *Journal of Safety Research, 38*, 643–650. https://doi.org/10.1016/j.jsr.2007.07.005.

Taylor, S. G., & Kluemper, D. H. (2012). Linking perceptions of role stress and incivility to workplace aggression: The moderating role of personality. *Journal of Occupational Health Psychology, 17*(3), 316–329. https://doi.org/10.1037/a0028211.

Torkelson, E., Holm, K., Bäckström, M., & Schad, E. (2016). Factors contributing to the perpetration of

workplace incivility: The importance of organizational aspects and experiencing incivility from others. *Work and Stress, 30*(2), 115–131.

Trépanier, S.-G., Fernet, C., Austin, S., & Boudrias, V. (2015). Work environment antecedents of bullying: A review and integrative model applied to registered nurses. *International Journal of Nursing Studies, 55*, 85–97. https://doi.org/10.1016/j.ijnurstu.2015.10.001.

United States Department of Labor, Bureau of Labor Statistics, & Survey of Workplace Violence Prevention. (2005). Survey of workplace violence prevention, 2005. Retrieved from http://www.bls.gov/iif/oshwc/osnr0026.pdf

von Thiele Schwarz, U., Hasson, H., & Tafvelin, S. (2016). Leadership training as an occupational health intervention: Improved safety and sustained productivity. *Safety Science, 81*, 35–45. https://doi.org/10.1016/j.ssci.2015.07.020.

Further Reading

Holbrook, C. M., Bixler, D. E., Rugala, E. A., & Casteel, C. (2018). *Workplace violence: Issues in threat management*. New York: Routledge.

Kelloway, E. K., Barling, J., & Hurrell, J. J. (2006). *Handbook of workplace violence*. Thousand Oaks: Sage.

Workplace Violence: Sex-Related Crimes

Rifath Ali
Department of Safety, Security, and Emergency Management, College of Safety and Justice, Eastern Kentucky University, Richmond, KY, USA

Keywords

Workplace violence · Workplace rape · Workplace sexual assault · Criminal intent · Sex-related crimes · Workplaces Respond · Title VII · Civil Rights Act of 1964 · Risk assessment · Sexual harassment · Sexual harassment policy · Gender norms · Workplace safety · Culture of safety · Slow life history · Life history strategy · LHS · Extra-legal strategies · Targets · Barnes v. Train

Definition

Workplace violence is "...any physical assault, threatening behavior, or verbal abuse occurring in the work setting" (NIOSH 1996). The Workplaces Respond resource center defines workplace violence as a violent threat or the act of violence targeting a person who is working. Violence can vary from intimidating language to a murder committed by anyone, including coworkers and management (Futures n.d.).

Sexual harassment is *unsolicited* sexually leaning conduct by someone in the workplace. Sexual harassment is also defined as a form of discrimination and therefore is a sex-related crime under Title VII of the Civil Rights Act of 1964 (Woerner and Oswald 1990).

Introduction

Sex-related workplace violence is linked to sexual harassment and other sex-related crimes. With criminal intent, sexual violence can be perpetrated by a coworker or an individual who has no reasonable association in the workplace. Often, the malefactor is committing a separate crime besides the violence. Causal crime examples include shoplifting, robbery, and trespassing. Rare and more serious sex-related crimes include rape (CDC 2013).

Customer/client or client-on-worker workplace sex-related violence involves clients and family members. This type of violence occurs frequently but is not limited to medical settings or medically induced situations (CDC 2013).

Worker-on-worker sex-related crimes, including sexual harassment, are referred to as lateral or horizontal violence and are among the most underreported crimes. Less than 16% of women report sex-related crimes to the police, according to the National Online Resource Center on Violence Against Women. Statistics from the US Department of Justice Bureau of Justice Statistics indicate that rape and sexual assault were reported to police 24% of the time. This is the fewest declared when contrasted with other workplace violence crimes (Futures n.d.). Worker-on-worker

violence often targets co-workers seen as "lower on the food chain," as with a supervisor to a subordinate (CDC 2013).

Personal relationship workplace violence is when the offender is in a personal relationship to a worker and violence happens at the workplace. With threats and violence, the consequences can also be against coworkers (CDC 2013). Workplace violence is connected to personal relationships in nearly one-fourth of instances. The typical situation involves a current or former romantic partner with workplace access who commits a sex-related crime of violence targeting an employee or customer (Futures n.d.).

Sexual violence is a workplace danger when anyone making contact with the workplace engages in sexually bullying or criminal behavior. The offender may be someone familiar or unfamiliar with the victim, such as a supervisor, co-worker, past or present dating partner, company client, or stranger. Sexual violence crimes vary from state to state but include rape, assault and battery, threats, sexual harassment, and unsolicited sexual touching (Futures 2017).

Osterburg and Ward (2013) point out that, due to a changing social environment, there are new types of sexual violence crimes in the workplace. Sexual exploitation of women, including the crime of rape, is facilitated by the growth of online technology and communication. Nearly all sex-related offenses require special attention and compassion, beginning with interviewing victims, witnesses, and even offenders require a high level of compassion and skill (Osterburg and Ward 2013).

Sexual harassment emerged as an issue when women entered the workplace, no longer working solely at home. Extensive studies disclose half of the women are sexually harassed while in their academic years or during their working career. Studies reveal that sexual harassment is terrifying, degrading, and at times physically violent. Harassment often continues for a long time and can cause acute psychological, health, and employment consequences. These issues have prompted social policy research and legislation (Fitzgerald 1993).

Criminal Intent with Sex-Related Workplace Violence

With criminal intent, as mentioned, sex-related crimes can be committed by someone with or without association with the workplace. The offender is often trying to carry out a separate crime concurrent with a sex-related workplace violence act. For example, a company parking garage mugging became a rape (CDC 2013). The leading cause of workplace homicides began with other criminal intent, according to a study by Tiesman et al. (2012).

Sex-Related Crimes

Sexual Assault

When she was finishing up her studies, Jenny Lee Corvo (2018) was directing a play and went to an associated hair stylist, the business owner. After his last stylist left, the man locked the salon door and began to cut Jenny's hair. When the owner brushed hair clippings off the salon cape, off Jenny's breasts, her fears and suspicions were confirmed. He held the cutting shears to her throat and proceeded to press against her and grope her private body areas. Gratified, he took payment for the haircut and let her out the door. Shook, Jenny tried to file a police report but was told she was not believable (Corvo 2018).

Rape

Mary St. Clair from Oakland, now a social worker, was raped when she was in the military by an officer. She did not report the crime out of shame and fear (Mosley et al. 2017).

Worker-on-Worker: Sex-Related Workplace Violence

The first sex-related worker-on-worker legal case was not until 10 years after passage of the Civil Rights Act, *Barnes v. Train* (1974). The plaintiff claimed she was terminated from her job for refusing to have an affair with her supervisor.

The case won on appeal after it was first dismissed (Woerner and Oswald 1990).

Haley Dillon et al. (2015) examined how differences between individuals are systemically related to different perceptions of sexual harassment. With its psychological and economic consequences, sex-related crimes are an important societal issue but difficult to define because of their subjective perception. Depending on one's gender and life history strategy (LHS), or background, sexual harassment resulted in significantly poorer life performance, including in the workplace. Those with a slow life history were more reticent and deeply affected (Dillon et al. 2015).

There are major, precedent legal cases concerning sex-related crime in the workplace. However, Paula McDonald et al. (2011) concluded through their research that there had been a reluctance in the workplace to seek avenues of redress and justice when violated by a sex-related crime. This is in spite of traditional and specific legal paths to follow when responding to sexual harassment. Using prevalence survey research, McDonald et al. (2011) reported that extra-legal strategies, the somewhat hidden but continual action of all organization types, do not tolerate reporting of worker-on-worker, sex-related crimes. Targets, or those who have been victimized by sexual harassment, are to use formal organizational grievance procedures or informal means to resist or redress sex-related crimes. Most targets do not officially report sex-related crimes due to reprisal fear or believing the grievance would not be taken seriously. Nonetheless, targets will seek assistance on their own or use informal, proactive, assertive options (McDonald et al. 2011).

Customer/Client: Sex-Related Workplace Violence

Kathleen McPhaul and Jane Lipscomb (2011) researched policy progress for the previous decade to document a state-wide mental health facility method to lower violence and violence threats. The overwhelming majority of workplace violence threats, including sex-related crimes, to caregivers and other health care workers, came from patients. Workplace violence comprises abuse, bullying, psychological violence, physical violence, racial aggravation, and sex-related crimes. Those interactions can include co-workers, supervisors, patients, families, visitors, and strangers (Cooper and Swanson 2002; International Council of Nurses 2000; McPhaul and Lipscomb 2011).

Personal Relationship: Sex-Related Workplace Violence

According to Barry Schwartz and Gary Srebrolow (2018), when working in close proximity to other employees, there can sometimes develop mutual attractions. This is the definition of the personal workplace relationship, which carries with it the danger of the relationship disrupting the workplace environment. For example, favoritism can be suspected by other employees or, if the relationship breaks down, there is tension and possibly a wrongful dismissal triggering a lawsuit and harassment complaint. The complaint is a sex-related crime if the offer and enticements connected to sexual favors, even if due to the personal relationship, are unwanted (Schwartz and Srebrolow 2018).

Workplace personal relationships can be a trigger for sex-related crimes of workplace violence from another employee. Even though little is known about the mind and mentality of the attacker who is also an employee, one reason is commonality at work (Holmes 1993).

Conclusion

In employment settings, there is a different risk assessment for sexual harassment and workplace violence, depending on management and its understanding of the types of sex-related violence to which the labor force, especially women, are likely to be subjected while working. Mitigating factors include the overall mental and physical health of workers and their well-being, morale, and sense of job satisfaction. All of these dynamics are also

directly related to organizational costs and productivity (Hatch-Maillette and Scalora 2002).

Sexual harassment laws, intended to reduce sex-related crimes, have produced significant changes in the workplace at the organization level. However, the implementation of sexual harassment laws has caused a backlash against management that initiates the regulations. According to research by Justine Tinkler (2013), sex-related workplace guidelines increase gender inequality attitudes between men and women, compelled by long-standing gender collaboration customs. Also, varying male and female hierarchical positions in the organization yielded unique but correlated concerns about status pressures caused by sexual harassment policies. Workplace regulations are intended to reduce inequality between social and gender groups. More studies are needed that analyze sex-related crime prevention laws and the social psychological processes they impact (Tinkler 2013).

Management perceptions and decision making in avoiding possible sex-related crimes in the workplace focus, particularly on gender. The female workforce usually has subjectively different circumstances when employed in traditional male workshops. Concerning sex-related crimes in the workplace, it is, therefore "mutually beneficial" for management and employees to assess the culture of safety and judgment of risk (Hatch-Maillette and Scalora 2002).

Cross-References

- ▶ Investigations: Sexual Assault
- ▶ Workplace Violence: Assault
- ▶ Workplace Violence: Intimate Partner Violence
- ▶ Workplace: Sexual Harassment

References

Barnes v. Train. (1974). District of Columbia.

CDC. (2013). *Workplace violence types*. Downloaded from https://wwwn.cdc.gov/wpvhc/Course.aspx/Slide/Unit1_5

Cooper, C. L., & Swanson, N. (2002). *Workplace violence in the health sector: State of the art*. International Labour Organization. https://www.who.int/violence_injury_prevention/injury/en/WVstateart.pdf

Corvo, J. L. (2018). *Why i froze and smiled during my sexual assault.* Medium. Psychology. Downloaded from https://medium.com/s/story/why-i-silently-froze-and-smiled-during-my-sexual-assault-7bf5d56deebc

Dillon, H. M., Adair, L. E., & Brase, G. L. (2015). A threatening exchange: Gender and life history strategy predict perceptions and reasoning about sexual harassment. *Personality and Individual Differences, 72* (January), 195–199. Downloaded from https://www.sciencedirect.com/science/article/pii/S0191886914005030#kg005

Fitzgerald, L. F. (1993). Sexual harassment: Violence against women in the workplace. *American Psychologist, 48*(10), 1070–1076. https://doi.org/10.1037/0003-066X.48.10.1070.

Futures Without Violence. (2017). *Why is gender-based violence a workplace issue?* Workplaces respond to domestic & sexual violence national resource center. Downloaded from https://www.workplacesrespond.org/wp-content/uploads/2017/01/Why-Is-Gender-Based-Violence-A-Workplace-Issue.pdf

Futures Without Violence. (n.d.). *The facts on gender-based workplace violence.* Workplaces respond to domestic & sexual violence national resource center. Downloaded from https://www.workplacesrespond.org/resource-library/facts-gender-based-workplace-violence/

Hatch-Maillette, M. A., & Scalora, M. J. (2002). Gender, sexual harassment, workplace violence, and risk assessment: Convergence around psychiatric staff's perceptions of personal safety. *Aggression and Violent Behavior, 7*(3), 271–291. Downloaded from https://www.sciencedirect.com/science/article/pii/S135917890100043X

Holmes, R. M. (1993). Stalking in America: Types and methods of criminal stalkers. *Journal of Contemporary Criminal Justice, 9*(4). Downloaded from https://journals.sagepub.com/doi/abs/10.1177/104398629300900404?journalCode=ccja

International Council of Nurses. (2000). *Position statement: Abuse and violence against nursing personnel*. Downloaded from www.icn.ch/psviolence00.htm

McDonald, P., Charlesworth, S., & Cerise, S. (2011). Below the "tip of the iceberg": Extra-legal responses to workplace sexual harassment. *Women's Studies International Forum, 34*(4), 278–289. Downloaded from https://www.sciencedirect.com/science/article/abs/pii/S0277539511000525

McPhaul, K. M., & Lipscomb, J. A. (2011). Workplace violence in health care: Recognized but not regulated. *The Online Journal of Issues in Nursing, 92004*(3), 1–14. Downloaded from http://ldihealtheconomist.com/media/nv09.pdf

Mosley, T., Leitsinger, M., Cheng, M., & Levi, R. (2017). *'I don't feel safe at work': Your #MeToo stories*. KQED News. Downloaded from https://www.kqed.org/news/11634433/i-dont-feel-safe-at-work-your-metoo-stories

NIOSH. (1996). Violence in the workplace. *Current Intelligence Bulletin, 57*. Downloaded from https://www.cdc.gov/niosh/docs/96-100/

Osterburg, J. W., & Ward, R. H. (2013). *Criminal investigation: A method for reconstructing the past* (6th edn). Taylor & Francis/ScienceDirect. Downloaded from https://www.sciencedirect.com/science/article/pii/B9781422463284500335

Schwartz, B., & Srebrolow, G. (2018). *#MeToo and the potential for sexual harassment claims in dental workplaces.* University of British Columbia. Downloaded from https://www.researchgate.net/profile/Barry_Schwartz2/publication/323945625_MeToo_and_the_Potential_for_Sexual_harassment_Claims_in_Dental_Workplaces/links/5ab3e93caca272171003c53b/MeToo-and-the-Potential-for-Sexual-harassment-Claims-in-Dental-Workplaces.pdf

Tiesman, H. M., Gurka, K. K., Konda, S., Coben, J. H., & Amandus, H. E. (2012). *Workplace homicides among U.S. women: The role of intimate partner violence*. NCBI HHS. Downloaded from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4687019/

Tinkler, J. E. (2013). How do sexual harassment policies shape gender beliefs? An exploration of the moderating effects of norm adherence and gender. *Social Science Research, 42*(5), 1269–1283. Downloaded from https://www.sciencedirect.com/science/article/pii/S0049089X13000811

Woerner, W. L., & Oswald, S. L. (1990) Sexual harassment in the workplace: A view through the eyes of the courts. *Labor Law Journal, 41*(11). Downloaded from https://search.proquest.com/openview/0deac54b96eac205ca9103ef51ca4b2a/1?pq-origsite=gscholar&cbl=1816463

Further Reading

Fitzgerald, L. F. (1993). Sexual harassment: Violence against women in the workplace. *American Psychologist, 48*(10), 1070–1076. https://doi.org/10.1037/0003-066X.48.10.1070.

Futures Without Violence. (2017). *Why is gender-based violence a workplace issue?* Workplaces respond to domestic & sexual violence national resource center. Downloaded from https://www.workplacesrespond.org/wp-content/uploads/2017/01/Why-Is-Gender-Based-Violence-A-Workplace-Issue.pdf

Futures Without Violence. (n.d.). *The facts on gender-based workplace violence.* Workplaces respond to domestic & sexual violence national resource center. Downloaded from https://www.workplacesrespond.org/resource-library/facts-gender-based-workplace-violence/

McDonald, P., Charlesworth, S., & Cerisec, S. (2011). Below the "tip of the iceberg": Extra-legal responses to workplace sexual harassment. *Women's Studies International Forum, 34*(4), 278–289. Downloaded from https://www.sciencedirect.com/science/article/abs/pii/S0277539511000525

Schwartz, B., & Srebrolow, G. (2018). *#MeToo and the potential for sexual harassment claims in dental workplaces.* University of British Columbia. Downloaded from https://www.researchgate.net/profile/Barry_Schwartz2/publication/323945625_MeToo_and_the_Potential_for_Sexual_harassment_Claims_in_Dental_Workplaces/links/5ab3e93caca272171003c53b/MeToo-and-the-Potential-for-Sexual-harassment-Claims-in-Dental-Workplaces.pdf

This encyclopedia includes no entries for X, Y and Z.